WGS℠

THE SEDONA CONFERENCE®

International Overview of Discovery, Data Privacy & Disclosure Requirements

A Project of The Sedona Conference® Working Group on International Electronic Information Management, Discovery & Disclosure

SEPTEMBER 2009 - PUBLIC COMMENT VERSION

The Sedona Conference® International Overview of Discovery, Data Privacy & Disclosure Requirements

A Project of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

Author:
The Sedona Conference®

Editor in Chief
Sean Regan

Managing Editors:
Richard G. Braman
M. James Daley
Kenneth J. Withers

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to Richard G. Braman, Executive Director of The Sedona Conference®, at rgb@sedonaconference.org or 1-866-860-6600.

The overview was prepared by the editors indicated; they do not necessarily represent the views of any of the individual editor's employers, clients, or any other organizations to which any of the editors belong nor do they necessarily represent official positions of The Sedona Conference®.

Thanks go to all who participated in preparing this *Overview*. In addition, we thank all of our Working Group Series℠ Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" Navigation bar on the homepage of our website.

Table of Contents

Table of Contents - Detailed

Introduction

Welcome to *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements.* [www.thesedonaconference.org]. This project of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6) provides an overview of the electronic discovery and data privacy landscapes of selected countries in both a standard and interactive format. An electronic version of this document is available at www.socialtext.net/wg-6

This is a companion resource to *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery (Public Comment Version 2008)*, which has been cited with approval by the European Commission's Article 29 Working Party in its Working Document 158 dealing with cross-border discovery.

Together, these publications are designed to provide a framework for constructive dialogue regarding the resolution (or at least mitigation) of cross-border discovery conflicts. This *Overview* resource is published in both a static and interactive wiki format that is managed by selected country editors to provide a platform for collaboration and dialogue, as well as a process for keeping information current.

Both *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements and The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery* represent the collective input of hundreds of members of WG6 from countries as diverse as Australia, Bermuda, Brazil, Canada, China, England & Wales, France, Germany, Ireland, Japan, Netherlands, South Africa, Spain, Switzerland, Sweden, United Kingdom and the United States, among others.

We want to thank the entire Working Group 6 for all their hard work, and especially the combined Steering and Editorial Committees. We also want to note that WG6 sought and received considerable assistance from members of The Sedona Conference® Working Group 1 in the United States, which began a similar process in October 2002 and published the first U.S. public comment draft of *The Sedona Principles* in March 2003. That publication and the editions that followed have been well received by U.S. courts, both as resources cited in judicial opinions and as significant contributions to the process leading to the amending of the Federal Rules of Civil Procedure in December 2006. We hope that *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements*, in conjunction with *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts* will make similarly positive contributions to the development of International law, policy and practice.

We also want to thank the Annual and Sustaining Sponsors of the Working Group Series; without their financial support our Working Groups could not accomplish their goals. They are listed at www.thesedonaconference.org/sponsorship.

To offer your help as a country editor or contributor or to make other suggestions for use or expansion of the *Overview*, or for further information about The Sedona Conference®, its Conferences or Working Groups, please go to www.thesedonaconference.org or contact us at rgb@sedonaconference.org.

Richard G. Braman
Excutive Director

Working Group 6 Steering Committee:

Quentin Archer (UK) Co-Chair
Steven C. Bennett (US)
M. James Daley (US) Co-Chair
Janet Lambert (UK)
Neil Mirchandani (UK)
Sandra Potter (AU)
Paul R. Robertson (US)

Australia

Sandra Potter - ***Lead Editor***
Derek Begg - ***Contributing Editor***
Sarah Sherwood - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   The High Court of Australia (the highest court in Australia, with original and appellate jurisdiction), the Federal Court of Australia and each of the State and Territory Supreme Courts have their own set of procedural rules and regulations, made under each court's governing Act, together with practice notes (also called practice directions) issued by the court. Though not uniform, there is predominant similarity between the jurisdictions. Court proceedings, including the admitting of evidence, and disclosure and discovery obligations are governed by these procedural rules, and in some instances, case law.

   The law relating to discovery or disclosure is governed by the rules of the court of the jurisdiction in which the discovery is taking place. In addition, a substantial body of case law has been developed dealing with the various aspects of the discovery process.

   A number of the courts' practice notes and practice directions provide guidance to parties on the practical processes the court expects them to follow in making discovery, including e-discovery. Practice notes and practice directions issued by Australian courts generally do not have the force of law, but are issued in exercise of the courts' inherent powers to regulate their own practice and procedure. As a result, compliance with practice notes and directions is not mandatory but is nonetheless routine.

   The form of discovery or disclosure in civil proceedings in Australian courts follows the common law model.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   There is substantial variation between Australian jurisdictions in relation to the obligations and procedure for making discovery or disclosure and whether discovery is general or to be limited in some manner.

   In ACT, Tas, Vic and WA the parties are entitled to mutual discovery without the need to obtain an order from the court. A party may be required, by written notice, to give discovery or disclosure to another party of all documents which are or have been in the party's possession, custody, or power relating to any questions raised by the pleadings filed in the proceedings. In certain States (NT, SA and Qld) discovery is mandatory if there are pleadings or if a claim has been filed.

   In the Federal Court and NSW, an order for discovery must be obtained from the court. In NSW, general discovery is not available. The court may only grant an order for discovery of specific classes of documents, or

on specific issues or questions. Most jurisdictions require or encourage the parties to give discovery only of limited categories of documents as agreed by the parties or determined by the court, to limit unnecessary and burdensome discovery. All superior courts, however, have the discretion to make orders in relation to discovery or disclosure where necessary.

Generally, the time to give discovery or disclosure is within a specified period after the close of pleadings, service of notice or making of an order for discovery.

The mode of discovery is by the filing at court and/or service on the requesting/opposing party, or exchange of, a list or affidavit of documents in an approved form. The list of documents may be accompanied by an affidavit verifying its completeness to the best of the deponent's knowledge, information and belief. Once again the procedural obligations vary between the jurisdictions.

The party is required to make reasonable searches and enquiries to identify all discoverable documents. What are reasonable enquiries depends on the circumstances in each case (*Re McGorm; Ex parte Co-op Building Society of South Australia (1989) 20 F.C.R. 387*). The Federal Court is the only jurisdiction which has attempted to regulate the obligation to search. A party must make a reasonable search, and in doing so may take into account the nature and complexity of the proceedings, the number of documents involved, the ease and cost of retrieval and the significance of a document. Most jurisdictions place a considerable obligation on solicitors as having the primary responsibility to ensure that their clients understand the importance of discovery and their duty to make discovery.

Where discoverable documents are destroyed or moved out of a party's possession before the commencement of the proceedings, the party responsible for the document destruction is required to describe the documents no longer in its possession and explain what has become of them.

The duty of discovery is a continuing one. A party is required not only to disclose discoverable documents as at the date the list or affidavit of documents was made, but also discoverable documents which subsequently come into existence, or whose existence subsequently comes to light. The duty of disclosure continues until the cause of action is determined and/or an allegation no longer remains in issue. A party's obligations in respect of discoverable documents that have subsequently come into its possession, custody or power are discharged by the filing of a supplementary list.

Failure to make proper discovery of documents may warrant dismissal or striking out of the defence if that failure has rendered it impossible to conduct a fair trial even if that conduct did not constitute a contempt of court. The suppression of a discoverable document, in spite of its later production, may attract such a sanction if it were no longer possible to remedy the consequences of suppression.

The documents to which disclosure does not apply are those where there is a valid claim of privilege, or which relate only to the credit of the individual who may testify at trial, or relate to instructions to or advice from counsel. The most common categories of privilege to be claimed are where a document was brought into existence for the purpose of seeking or giving legal advice or in anticipation of litigation. A claim of privilege is made by affidavit.

The obligation to give discovery is generally discharged by the party giving discovery producing the documents on the list or affidavit for which no objection to production has been made, and the party seeking discovery inspecting the documents and being permitted to take copies.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

The rules in the majority of Australian jurisdictions provide for pre-action disclosure (known as preliminary discovery) to enable a plaintiff to identify a potential defendant or to obtain documents from the prospective defendant which might assist the plaintiff to establish the basis of a cause of action.

A party may, after making all reasonable enquiries, apply to the court for an order for preliminary discovery to establish the identity or whereabouts of a potential defendant. Similarly, a party who, after making all relevant enquiries, does not have sufficient information to decide whether to commence proceedings, may apply to the court for an order requiring discovery from a potential defendant. The court may make an order if it is satisfied that the applicant has reasonable cause to believe that there may be a right of relief against that person, and that the person may possess or have possessed documents, inspection of which would assist the applicant to make a decision.

Preliminary discovery is also available to give the applicant documents to assist in framing a cause of action against an identified prospective defendant. Where the applicant has made all relevant enquiries, and does not have sufficient information to decide whether to commence proceedings, and it appears that the prospective defendant is likely to have documents tending to assist this enquiry, the party may apply to the court for an order requiring discovery from that person.

On such an application, an order may be made if the court is satisfied that the applicant has reasonable cause to believe that there may be a right of relief against that person, and that the person may possess or have possessed documents, inspection of which would assist the applicant to make a decision.

The applicant is not required to show a good cause of action (*Prosnow International Pty. Ltd. v. Polar Technologies Pty. Ltd. & Polar Technologies International Pty. Ltd. (1997) 39 I.P.R. 369*), a prima facie case (*NRMA v. John Fairfax Publications Pty. Ltd. 2002 N.S.W.S.C. 563*), or likelihood that relief can be obtained against the respondent (*Pacific Dunlop Ltd. v. Australian Rubber Gloves Pty. Ltd. (1992) 23 I.P.R. 456*). The evidence, although falling short of establishing all the ingredients of a prime facie case, may point sufficiently to the existence of a case for relief as to make it proper, in the interests of justice, that preliminary discovery be ordered so that proceedings for that relief can be brought.

In all cases the court's power is discretionary and an order will only be made when it is reasonably necessary for the proper administration of justice, bearing in mind that a serious invasion of privacy and confidentiality may be involved before it is clear that there is an issue to litigate (*McCarthy v. Dolpag Pty. Ltd. (2000) W.A.S.C. 106*).

The court rules in a number of Australian jurisdictions also provide a means of obtaining discovery during the proceedings from a person or entity who is not a party to the proceedings. In general, the courts will only exercise their power to make such orders against non-parties in exceptional circumstances. The courts exercise caution in this area because of the fact that the non-party has no necessary connection with the litigation other than the possession of documents, it may be expensive in terms of both monetary cost and case management time, and there is an alternative process available for parties to proceedings to obtain documents from a non party, namely the issue of a subpoena.

The courts may exercise their discretion to order non-party discovery in circumstances where: there is a real likelihood that the documents for which discovery is sought will advance the case of the applicant, or damage the case of the applicant's opponent in the proceedings; the applicant has been refused inspection of the documents; the information contained in the documents cannot be obtained from any other source; or if the party were not to have access to the trial the value of the information sought would be lost or seriously diminished.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The general position in Australia is that owners of documents are entitled to deal with their documents as they choose (*Registrar of the Supreme Court, Equity Division v. McPherson and Others (1980) 1 N.S.W.L.R. 668*), subject to certain statutory requirements for the retention of documents (such as business and taxation records) for specified periods.

While there is no provision in the rules of court at either a Federal or State level for a party to retain or preserve documents for the purpose of civil litigation, in 2006 Victoria passed the Crimes (Document Destruction) Act 2006 (Vic) which added new provisions to the State's principal criminal statute, the Crimes Act 1958 (Vic),[1] and makes it a criminal offence to destroy a document or thing that is, or is reasonably likely to be required as evidence in a legal proceeding. Where the person is an officer of a company, the company is exposed to prosecution directly. The Act was designed to prevent, in the gap between court cases, the precipitous destruction of evidence identified as relevant in a particular type of proceedings and therefore likely to be required in future cases of the same kind.

This legislation is supported by the Evidence (Document Unavailability) Act 2006 (Vic), now incorporated within the Evidence Act 2008 (Vic), which effectively allows Victorian Courts and Tribunals to intervene in civil proceedings where relevant documents are "unavailable" (in that they have been lost or destroyed) to ensure a fair outcome between the parties. It achieves this by giving courts power to make orders such as drawing an adverse inference from the unavailability of the document, altering the burden of proof of a fact in issue between the parties, and restricting the use of other evidence.[2]

These statutes were enacted following decisions of the Supreme Court of Victoria and the Court of Appeal in *McCabe v. British American Tobacco Australia Services Ltd. (2002) V.S.C. 73* and *British American Tobacco Australia Services Ltd v. Cowell (as representing the Estate of Rolah Ann McCabe) (2002) V.S.C.A. 197*. The primary relevance of these proceedings in relation to discovery obligations is the legal consequences of document destruction before the commencement of proceedings.

The case arose out of a claim against a tobacco manufacturer alleged to have caused the plaintiff's lung cancer. Before the trial, the defendant admitted that it had destroyed potentially discoverable documents in accordance with its document retention/destruction programme at a time when litigation was apprehended. The plaintiff argued that as a result a fair trial was impossible.

At first instance the judge held that a duty to preserve documents existed even though litigation was only anticipated. He found that the defendant's document retention policy was created in anticipation that there would be litigation against it, and that the destruction of potentially relevant documents prior to the

[1]Crimes Act 1958 (Vic), s. 253-255.
[2]Evidence Act 2008 (Vic), s. 169, Dictionary Part 2 Clause 5 "Unavailability of Documents and Things".

commencement of proceedings had been done so as to prevent the plaintiff receiving a fair trial. An application to strike out the defence was granted because the process of discovery had been deliberately subverted.

The decision was overruled by the Court of Appeal on the basis that the deficiencies in discovery were not sufficient as to warrant the striking out of the defence. An order to amend the discovery affidavit should have been made, so that it indicated what had happened to the documents handled under the document retention programme. In considering the need for a balance to be struck between the right of any company to manage its own documents, and the right of a litigant to have recourse to the documents of the other side, the court found that the criterion for judicial intervention is whether the conduct of a party in destroying documents before the commencement of the litigation amounts to an attempt to pervert the course of justice or contempt of court (meaning criminal contempt).

In this context, reference should be made to the activities and recent recommendations of the Public Records Office Victoria ("PROV"), the archiving authority for Victoria. The PROV has established standards for the management of public sector records, and issues advice on their application. Most significantly, the PROV has issued formal advice to Victorian government agencies on the record keeping implications of the Crimes (Document Destruction) Act 2006 (Vic) and the Evidence (Document Unavailability) Act 2006 (Vic) with general principles and recommendations for management of public records. PROV advises that:

> Victorian Government agencies, as with other organisations, must be aware of the extent and implications of the legislation. All agencies will be most likely to avoid liability under the Act if:
>
> 1. they create effective, comprehensive records management systems and policies, supported by a corporate culture that does not countenance the illegal destruction of records, and
>
> 2. they provide training for all staff involved in records disposal. Agencies in particularly litigious areas of business may need to exercise even greater caution in destroying records related to activities that may potentially give rise to lawsuits.
>
> Agencies must be aware that while the Act does *not* criminalise normal records disposal (including disposal formally authorised under a relevant Public Record Office Victoria Retention & Disposal Authority, or RDA), it will *not* be possible to use an RDA to legalise or justify the destruction of documents or records where that destruction meets all the criteria for the offence.[3]

Once legal proceedings have commenced, documents should not be destroyed if they could be considered relevant to the litigation *(Rockwell Machine Tool v. EP Barrus (Concessionaires)* Ltd. (1968) 2 *All* E.R. 98). The solicitors involved in a case have a positive duty to explain to their clients at an early stage of the proceedings the requirements of discovery and the importance of not destroying documents which might possibly have to be discovered. In New South Wales, lawyers who destroy relevant records, or advise clients to do so, are at risk of disciplinary proceedings for professional misconduct.

Once notices or orders requiring discovery have been issued, parties are obliged to preserve documents which are the subject of such orders or notices. In view of recent case law it appears prudent that if either litigation is anticipated or proceedings have been commenced but the discovery process has not yet been initiated, a party should preserve documents which may have potential relevance to the proceedings.

[3]Public Records Office Victoria, PROA 06/18: Advice to Agencies 18: Crimes (Document Destruction) Act 2006: Implications for Government Recordkeeping (April 2007), p.4.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

Parties to litigation are under an obligation to make proper discovery, and failure to do so may attract sanctions.

Apart from the courts' inherent jurisdiction to make any order it considers appropriate against a party who fails to comply with its discovery obligations, court rules provide a range of specific sanctions. The possible consequences of destroying documents relevant to litigation after the commencement of proceedings include breach of discovery obligations; adverse inferences drawn against the party responsible for the destruction of documents; contempt of court; perverting the course of justice; breaches of the various criminal statutes and sanctions against the solicitors involved.

As discussed in question 4 above, the destruction of documents before litigation has commenced may amount to an attempt to pervert the course of justice or a criminal contempt, and attract the sanction of dismissal of the proceedings or striking out all or part of the defence, in circumstances where the court concludes it is not possible to have a fair trial of a proceeding because of the destruction of the documents (*British American Tobacco v. Cowell*, above). In Vic, the crime of destroying evidence now exists, under the Crimes (Document Destruction) Act 2006 (Vic) also referred to in question 4 above.

Corporate document retention/destruction policies were recently addressed in civil proceedings in the Federal Court, and indicate the seriousness with which the courts view the obligations of legal advisers to make proper discovery (*Seven Network Ltd. v. News Ltd. (2007) F.C.A. 1062, paragraphs 482 - 490*).

One of the parties to the proceedings, and particularly its Chief General Counsel, had actively pursued a policy of expediently deleting the majority of his electronic communications, partly to prevent their disclosure in litigation.

While the presiding judge declined to impose any sanction on the organisation itself, he found that any failure on its part to take action against its Chief General Counsel "would reflect very seriously indeed on (the party's) standards of commercial morality" (paragraph 39).

The "deliberately dishonest conduct" of the solicitor concerned (paragraph 425) was referred by the court to the solicitors' regulatory body, the Law Society of New South Wales, for its consideration and referral, and if appropriate, to the solicitors' professional disciplinary body. The possible outcomes of such action are serious and may include the suspension or cancellation of a solicitor's practising certificate.

The Evidence Act 2008 (Vic) empowers Victorian courts to make certain sanctions. These are discussed in question 4 above.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

In Australia, legal costs in civil proceedings are borne initially by each party. At judgment the award of costs is at the discretion of the court. The usual exercise of this discretion is that costs "follow the event." That is, the successful party's costs are paid by the loser. Once an award of costs has been made, the amount is assessed against issues of necessity or reasonableness in the circumstances of the case, and items of legal work being calculated generally by reference to a scale set by the court.

The costs of discovery or disclosure are treated in the same manner, that is, each party is responsible for their own costs incurred in making discovery subject to an order from the court.

The courts in most jurisdictions have costs provisions relating to preliminary discovery, which gives them the discretion to make orders regarding the parties' costs of making/opposing the application and the non-party's or respondent's costs of compliance with the order.

Practice Notes in relation to information technology issued recently by several Supreme Courts and the Federal Court indicate growing judicial concern with aspects of the discovery process and the particular costs issues arising from discovery of electronic material. A number of these guidelines anticipate that the party demanding discovery of electronic material may be required to bear the costs of the party making discovery or that the costs associated with providing access to hardware, software or other resources to make inspection of original electronic material should be agreed between the parties.

In NSW, the costs of discovery that are recoverable may be limited to ensure the most cost efficient method of the discovery process. In Vic, the Supreme Court has acknowledged that the reasonable costs of complying with the requirements of its Practice Notes, including the expenses of retaining necessary external service providers, are a proper part of the legal costs that may be claimed at judgment. The Federal Court, in its most recent technology Practice Note (issued in 2009), emphasized cost as a factor in the reasonableness of discovery searches, observing that "electronic documents must be managed efficiently to minimize the cost of discovery and the cost of the trial."[4] These issues are discussed further in answer to question 16 below.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

The extent of the obligation regarding the discovery of electronically stored information ("ESI") is still developing in Australia. Australian laws generally use the term "document" to describe any piece of information or communication which is potentially discoverable, in whatever form or storage medium. This will be dealt with in question 8 below.

The courts have begun to address the application of discovery procedures to electronic documents. Recent case law has established that electronically stored information on CD-ROMs and computer hard drives is subject to the discovery process (Sony Music (Aust.) Ltd. v. University of Tasmania (2003) 198 A.L.R. 367). It has also been held that e-mail records and back-up tapes are discoverable (*N.T. Power Generation Pty. Ltd. v. Power and Water Authority* (1999) F.C.A. 1669).

In addition, legislative provisions in most jurisdictions have been expanded, in differing degrees, in order to embrace current developments in electronic document storage, processing and retrieval. The Federal Court and six Supreme Courts have also issued Practice Notes/Directions or Guidelines on the use of information technology in civil litigation. Through these Guidelines, some Courts are not limiting the use of technology to the discovery process but are encouraging parties to continue the management of discovered documents electronically right through to the hearing.[5] The use of technology by lawyers to manage and list disclosed documents, those obtained by way of inspection or produced by third parties, has been steadily increasing. This

[4]Practice Note 17, paragraph 5.1(b).
[5]Technical Guide for Preparing and Submitting Documents for E-Trials (2008), see Practice Note 17 (2009).

trend has been particularly obvious in large, multi-party or complex litigations in which information technology has come to play a vital role and is now increasing as court guidelines are revised and reissued to match technological developments and electronic document management practices.

For some time, leading Australian litigators have considered it essential that any discovery include a plan for discovering electronic documents. The Federal Court now expects parties to have discussed and agreed upon a practical, cost-effective and proportional discovery plan before an order for discovery will be made.[6]

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

All court rules in Australia attach the discovery obligation to any material that meets their respective definitions of the word "documents."

All Australian jurisdictions have statutory definitions of the word "document" that have attempted to acknowledge, to some degree, the increased use of information technology. In particular, s. 25 of the Acts Interpretation Act 1901 (Cth) extends the conventional meaning to include "any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device"; and the Evidence Act 1995 (Cth), which has been adopted in a number of State jurisdictions, defines a document as "any record of information" including electronic data.

Statutory provisions in most jurisdictions have variously expanded the definition to include a record of information, not only paper but anything from which sounds, images or writings can be reproduced, such as data stored on tape, video or computer, disc, sound track, film, negative or other device in which sounds or other data are embodied.

In a recently updated Practice Note in NSW the term "ESI" has been defined as meaning electronically stored information and includes emails, web pages, word processing files, images, sound recordings, videos and databases stored in any device.

In the Federal Court's recently updated Practice Note, "electronic document" is defined as "a document or component of information that was originally created using a computer system, software application or database." Metadata embedded within an electronic document is considered part of the document. The definition includes an email, email attachment or a "loose file" – an electronic document that is stored in its native form in a "container" (an electronic document store) that is a file system or directory system but not an email box. A container is specifically excluded from the definition.[7]

The inclusion of irrelevant material in the storage medium does not mean that the information should not be discovered (*Sony Music Entertainment (Aust) Ltd. v. University of Tasmania (2003) 198 A.L.R. 367*).

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

Strictly speaking, none of the Practice Notes and Guidelines that have been issued by the courts require the parties to meet and discuss electronic disclosure. Some Practice Notes expect the parties to meet and confer, and in these jurisdictions parties would need compelling reasons for not doing so, to avoid a court order directing them to do so (under the courts' inherent powers to control their own procedures).

So, whilst not strictly mandating the parties to meet and confer, the Practice Notes and Guidelines uniformly encourage the parties to meet as soon as possible after the commencement of the proceedings, for the purpose

[6]Practice Note 17, paragraph 6.1.

[7]See Glossary to Practice Note 17, http://www.fedcourt.gov.au/how/practice_notes_cj17_glossary.html.

of discussing the management of electronic documents and the use of technology in the proceedings. In NSW, there is an expectation by the court that the parties have met to confer on electronic discovery issues prior to any hearing relating to discovery. The primary responsibility to agree on the use of technology lies with the parties – in Vic, the Practice Note states this explicitly[8] – however the courts retain the discretion to make orders in this regard. The Federal Court is another jurisdiction that "expects" parties to meet and confer. In one division of the Supreme Court of NSW "the Court endorses a flexible rather than prescriptive approach to discovery to facilitate the making of orders to best suit each case."[9]

The Federal Court's Practice Directions state that the Court expects the parties to have met and conferred in order to discuss and agree upon a practical and cost-effective discovery plan,[10] and for the purpose of reaching an agreement about the protocols to be used for the electronic exchange of documents and other issues relating to efficient document management in a proceeding.[11] The Court has issued a checklist identifying issues that the parties are expected to consider, including the scope of discovery, reasonable search strategies, management of ESI, preservation strategies, timetables, cost, managing privilege claims, protocols and discovery issues where agreement is ultimately not reached.[12]

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

There is no legislation in Australia which specifically addresses the obligation to preserve documents which are in solely electronic form in relation to pending or possible litigation.

However, the upshot of the *McCabe* judgments, the ensuing Victorian legislation relating to document destruction and unavailability, and the PROV recommendations, all point to the potential existence of implicit obligations in both the public and private sector to preserve all documents and records related to pending or anticipated litigation.

The legal requirements regarding discovery generally and the preservation and destruction of documents in particular are addressed in questions 4 and 5 above.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

There are no legal provisions that specifically regulate the scope of the obligation to discover electronic documents. Certain courts have provided guidelines regarding the type of potentially discoverable material in electronic form which may be in the possession of a party, and as to matters that the parties should take into account in the collection, retention and production of electronic material.

As discussed in question 2, above, a party has an obligation at common law to make reasonable searches to identify all discoverable documents. The extent of the obligation to discover electronic documents is the same. As discussed in question 6 above, in some jurisdictions, the courts weigh the time, cost and the inconvenience of the discovery process against the relative importance of the documents sought. In making a reasonable search, a party must take into account the nature and complexity of the proceedings, the number of documents involved, the ease and cost of retrieving the document, the significance of any document likely to be found and any other relevant matter.

[8] Vic: Practice Note, 1 paragraph 2.4 (2007).
[9] NSW: Practice Note SC Eq 3, paragraph 27 (2007).
[10] Practice Note 17, paragraph 6.1.
[11] Id. at paragraph 7.1.
[12] See Practice Note17, Pre-Discovery Conference Checklist.

Whilst these obligations apply to the discovery process generally, practical issues surrounding the nature of ESI will affect the parties' ability to comply with these obligations in any particular case.

The Federal Court now expects parties to agree upon a strategy to ensure that electronic documents which are potentially discoverable documents are preserved in their original format.[13]

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

There is no specific legislation that requires a party to verify that a search has been made for electronic documents. The general discovery obligations discussed in question 2 above, requiring verification of an affidavit or list of documents apply equally to electronic documents.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

The courts in the majority of the Australian jurisdictions have issued Practice Notes or Guidelines promoting the use of information technology in civil proceedings. As part of the Practice Directions provided in these Practice Notes, parties are variously expected or encouraged to use information technology to create lists of discoverable documents, undertake discovery by exchanging electronic data created in accordance with an agreed protocol, and arrange for inspection of discovered material using information technology.

While the use of information technology is currently not mandatory at any stage of the proceedings in most states, the Federal Court expects parties to use information technology in this way where a significant number (in most cases, 200 or more) of the documents relevant to the proceeding have been created or are stored in an electronic format; and the use of technology in the management of documents and conduct of the proceeding will help facilitate the quick, inexpensive and efficient resolution of the matter.[14] The NSW Supreme Court has also recently flagged a more robust approach in certain commercial cases with the issue of a new Practice Note which requires discovery to be made electronically, and Court Books to be established in electronic form as the default position.

Included in a number of these Guidelines are information technology checklists (used to identify information technology issues that may arise during the proceedings), suggested fields of data parties should consider using to collect electronic data, glossaries of terms and, in certain cases, draft and default protocols for the exchange of electronic information.[15] Some courts have issued further general information to guide lawyers unfamiliar with the discovery of ESI.

Further movements are also being made regarding the use of technology in discovery and for document management at both a federal and state level. In March 2008, the Victorian Law Reform Commission released Report 14 entitled 'Civil Justice Review.' The report culminated in 177 recommendations for reform of the civil justice system in Victoria, including a number of recommendations regarding case management and the use of technology. The report also recommended the introduction of new pre-trial oral examinations (similar to U.S. style depositions) aimed at 'getting to the truth earlier and easier' through facilitating the pre-trial disclosure of relevant information and limiting the real issues in dispute. The report also recommended that the Victorian County and Magistrates' Courts could consider adopting the Vic Supreme Court's approach to e-litigation:

[13] Id. at paragraph 5.1.
[14] Practice Note 17, paragraph 1.3.
[15] *See, e.g.*, Practice Note 17, Default Document Management Protocol and Example Advanced Document Management Protocol.

> The Supreme Court's Practice Note encourages parties to consider the use of technology at the outset and thereby avoid problems at trial. The court's aim is to decrease document management problems through technology, thereby reducing costs and delay; and to encourage lawyers to consider the ways in which the use of technology might lead to the more efficient conduct of litigation.

The stated purpose of the Federal Court's 2009 revised Practice Note is to encourage and facilitate the effective use of technology in proceedings before the Court by setting out the Court's expectations of how technology should be used in the conduct of proceedings before it and recommending a framework for the management of documents electronically in the discovery process and the conduct of trials.[16]

To a lesser or greater extent, this is the overarching purpose of each of the Guidelines issued by Australian courts so far.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

The legal standard for these matters has been discussed in questions 2, 6 and 11 above.

To summarise the position, under Australian laws of evidence, electronic information falls within the various statutory definitions of "document." There are no legal provisions that specifically regulate the standard for accuracy and completeness specifically with respect to the processes of discovery of electronic documents.

A party has an obligation at common law to make reasonable searches to identify all discoverable documents, that is, all documents that are relevant irrespective of their form, whether electronic or otherwise. What is reasonable depends on a matrix of factors, which can include the nature and complexity of the proceedings, the number of documents involved, the ease and cost of retrieving the documents, and the significance of any document likely to be found.

Some courts have also indicated their expectations of parties with respect to the application of these obligations to the discovery of electronic documents. The Supreme Court of NSW:

> …Expects practitioners to have…given consideration to and conferred in relation to the particular issues involved in the collection, retention and protection of electronically stored information, including …whether the burden and cost involved in discovering a particular document or class of documents is justified having regard to the cost of accessing the document or class of documents and the importance or likely importance of the document or class of documents to the proceedings.

The Federal Court's expectations – as detailed in questions 9 and 13 above – can be seen to be very similar. The Court has implemented a regime where it expects parties to agree on strategies for the management of electronic documents, including their identification, collection, processing, analysis, review and exchange. Agreement on a strategy does not relieve the parties of their obligation to conduct a "reasonable search" in accordance with the Court's rules (see question 2).[17] However, whether the actual management of electronic information has been accurate or complete may depend on the extent to which a party has complied with the strategy that had been agreed.

[16] Practice Note 17, paragraph 2.1.

[17] Order 15, Rule 2(3) and (5). This general obligation is reinforced in Practice Note 17, paragraph 1.4.

A party is usually required to file an affidavit verifying the completeness of its list of discovered documents, to the best of the deponent's knowledge, information and belief. There is no separately defined standard of compliance with this obligation with respect to electronic documents.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

Loss or waiver of privilege through the inadvertent disclosure of privileged information at the pre-trial stage of proceedings is governed by the common law (*Australian Rugby Union Ltd. v. Hospitality Group (1999) 165 A.L.R. 253*). Whether or not inadvertent disclosure constitutes waiver of privilege over legal advice ("legal professional privilege" or "client legal privilege") depends upon whether the party claiming privilege has acted inconsistently with the privilege being maintained (*Man v. Cattrell (1999) 201 C.L.R. 1*).

In *GT Corporation Pty. Ltd. v. Amare Safety Limited (2007) V.S.C. 123*, the defendant in meeting its discovery obligations, inadvertently provided the plaintiff with copies of electronic documents over which the defendant then sought to claim privilege. The court held that the manner in which the defendant's electronic discovery had been provided (by a computer forensics organisation) without an index or means of identifying the documents or their origin, had contributed significantly to the subsequent problems.

Reference should be made here to s. 122 of the Evidence Act 1995 (Cth), which addresses the loss of client legal privilege, allowing evidence of privileged communications to be adduced at trial. The test of waiver for the purposes of this section is whether there has been sufficient disclosure to warrant the loss of privilege. It has been held, however that the Evidence Act does not apply to discovery and the inspection of documents (*Esso Australia Resources Ltd v Commissioner of Taxation (Cth) (1999) 201 CLR 49*).

In NSW, Practice Note No. SC Eq 3, which came into effect on 30 July 2007, signals the Supreme Court's intention to actively manage the costs associated with discovery and particularly the review of documents for privilege to their disclosure. The court specifically encourages the parties to consider the issue of inadvertent disclosure of privileged documents through electronic discovery processes. It suggests the possible adoption of discovery on a without prejudice basis, with a procedure for claiming privilege subsequent to discovery.

In the Federal Court, Practice Note 17 (updated in 2009) sets out the Court's expectations on the parties, who should agree upon the strategies they will use to manage documents that are subject to a claim of privilege or confidentiality, and/or ordered by the Court to be privileged or confidential.[18]

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

Costs are addressed, as previously noted in question 6, whether the information is electronic or otherwise.

In Australia, legal costs in civil proceedings are borne initially by each party. At judgment, the award of costs is made at the discretion of the court. The usual exercise of this discretion is that costs "follow the event," that is, the successful party's costs are paid by the loser. Once an award of costs has been made, the amount is assessed against issues of necessity or reasonableness in the circumstances of the case, and items of legal work being calculated generally by reference to a scale set by the court.

The costs of discovery or disclosure are treated in the same manner, that is, each party is responsible for their own costs incurred in making discovery subject to an order from the court.

[18]Practice Note 17, Pre-Discovery Conference Checklist, paragraph 7.1.

The courts in most jurisdictions have costs provisions relating to preliminary discovery, which gives them the discretion to make orders regarding the parties' costs of making/opposing the application and the non-party's or respondent's costs of compliance with the order.

Practice Notes in relation to information technology issued recently by several Supreme Courts indicate growing judicial concern with aspects of the discovery process and the particular costs issues arising from discovery of electronic material. A number of these Guidelines anticipate that the party demanding discovery of electronic material may be required to bear the costs of the party making discovery or that the costs associated with providing access to hardware, software or other resources to make inspection of original electronic material should be agreed between the parties.

In NSW, the costs of discovery that are recoverable may be limited to ensure the most cost efficient method of the discovery process.

In Vic, the Supreme Court has acknowledged that the reasonable costs of complying with the requirements of its Practice Note, including the expenses of retaining necessary external service providers, are a proper part of the legal costs that may be claimed at judgment.

In the Federal Court's revised Practice Note, sections on costs that were contemplated in the public discussion draft were not ultimately included. It contains no express provision for costs, which continue to be dealt with under the court's rules without any express provision regarding electronic disclosure.

Although the Practice Note is silent on costs, the Court expects parties to apply its Guidelines for the overarching purpose of "the just resolution of disputes as quickly, inexpensively and efficiently as possible."[19] This language strongly implies that appropriate costs incurred on electronic discovery and document management will be properly claimable, and that inefficient, inappropriate or excessively costly electronic processes may result in adverse costs orders.

Factors the Court would consider in deciding what are reasonable discovery costs are the same whether the processes are electronic or not: the nature and complexity of the proceedings, the number of documents involved, the ease and cost of retrieval and the significance of a document to the case.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

As discussed in question 4 above, Australia has certain statutory requirements for the retention of documents (such as business and taxation records) for specified periods, but there are no legal provisions whose broad focus is on the obligation to retain electronic documents for business purposes.

Information management policies and procedures are common in Australia for business purposes, although their prevalence, sophistication and compliance levels vary significantly.

The preservation of information generally for legal purposes is also discussed in question 4 above, and corporate document retention/destruction policies in particular are discussed in question 5 above.

The practice of issuing legal hold notices upon prospective parties to litigation is not yet common in Australia.

[19] Practice Note 17, paragraph 3.1 (2009).

Evidence may be preserved by court order where a party identifies that there is a real risk a defendant will either destroy evidence or place it outside the jurisdictional powers of the court. In these circumstances, the party may apply to the court for a search order or an "Anton Piller" order (after the case of *Anton Piller KG v. Manufacturing Processes Ltd. (1976) Ch 55*). This order allows the party to enter the defendant's premises and secure the evidence at risk.

The securing of electronic information under a search order is specifically contemplated by Practice Notes throughout Australian courts, which include provision for the appointment of independent computer specialists to image computer drives where required.

In cases to which the Federal Court's Practice Note applies, the Court expects parties to agree upon strategy to ensure that electronic documents that are potentially discoverable documents are preserved in their original format.[20]

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The use of electronic information management technologies for legal reasons in Australia was historically limited to major law firms and larger and multinational corporations. Practice Notes concerning the handling of electronic information in litigation and the corresponding use of information management technology began to be issued by Supreme and Federal Courts in the late 1990s with the specific intention of ensuring that technology would not become a barrier to accessing justice.

Current Practice Notes permit the electronic discovery of hard copy and electronic information and provide guidance on the use of technology to manage these processes efficiently and cost-effectively. Some of these Practice Notes communicate the expectations of courts that parties will have considered the use of electronic information management technologies in the process of litigation, particularly discovery.

The force with which the Courts have imposed electronic information management technologies on parties has varied. The current high point may be in cases to which the Federal Court's recently revised Practice Note applies, where the Court has introduced an electronic discovery regime with the express expectation that the parties and their representatives will cooperate with and assist the Court in fulfilling its overarching purpose – the just resolution of disputes as quickly, inexpensively and efficiently as possible – and, in particular, in identifying documents relevant to the dispute as early as possible and dealing with those documents in the most efficient way practicable.[21]

The practical effect of these Practice Notes has been to require parties and their lawyers to use electronic information management technologies as a necessity of litigation in many more cases. Accordingly, Australia is experiencing a period of growth in the uptake use of these technologies.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

Australian statutes that protect information privacy have been enacted at Federal and State level. The main Federal obligations regarding the protection of personal information are primarily contained in the Privacy Act 1988 (Cth). This Act regulates many aspects of the handling of "personal information" including collection, use, disclosure, quality, accuracy and security. It was originally introduced to require Federal public sector

[20]Practice Note 17, Pre-Discovery Conference Checklist, paragraph 5.1.
[21]Practice Note 17, paragraph 3.

agencies to comply with 11 Information Privacy Principles ("IPPs") when handling personal information, and it was extended in 2001 to impose similar obligations on a large section of the private sector through the introduction of 10 National Privacy Principles ("NPPs").

Both sets of Principles impose specific obligations at all stages of the personal information lifecycle, including the collection, storage, use, disclosure, quality and security of personal information and also provide for rights of access to the information.

The type of material protected by the privacy rules contained in the Act is "personal information." The Act defines "personal information" as:

> … Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Depending on the circumstances, this can include information about a person's name, date of birth, address, telephone number, family members, or any other information that could allow the person to be identified.

In addition to the protection of personal information, the Act imposes stricter levels of protection for the handling of "sensitive information" by private sector organisations. Sensitive information is a subcategory of personal information. It includes information about a person's health (including genetic information), racial or ethnic origin, political opinions, religious beliefs, professional or trade union memberships, sexual orientation or criminal history.

In respect of private sector organisations, the NPPs cover ten areas:

1) Collection
2) Use and disclosure
3) Data quality
4) Data security
5) Openness
6) Access and correction
7) Identifiers
8) Anonymity
9) Transborder data flows
10) Sensitive information

Once an organisation has collected information about an individual, and stored it as a record, the NPPs impose specific security obligations on the organisation, and rights of access for the individual whom the information is about. Access to the information can be refused on a number of grounds including:

a) if information relates to legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery;
b) denying access is required or authorised by or under law;
c) providing access would be unlawful.

In addition to the above requirements organisations bound by NPPs must not transfer the information to anyone (other than the organisation itself or the individual) in a foreign country, unless:

a) the individual consents to the transfer;

b) the recipient is subject to a law or other binding obligation which upholds principles that are substantially similar to the NPPs, or has taken steps to ensure that the information will not be processed inconsistently with the NPPs.

To date there has been little indication of the practical impact of Australian privacy legislation on the civil discovery process. Under the NPPs, organisations are not permitted to disclose personal information for purposes other than the primary purpose for which it was first collected unless, amongst other things, the use or disclosure is required or authorised by law.

In 2007, the NSW Court of Appeal held in *Roads & Traffic Authority of NSW v. Australian National Car Parks Pty. Ltd. (*2007) *N.S.W.C.A.* 114 that an order for preliminary discovery amounted to such a "disclosure" and commented that a response to a subpoena would have similar force. The case did not specifically discuss discovery generally, whether by court order or where sought as of right pursuant to the rules of court.

In addition, under NPP 4 sub-clause 4.2, an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2. In Vic, the PROV has advised that the destruction and/or permanent de-identification of public records, when their retention does not serve such a "purpose," would not be in contravention of the Crimes (Document Destruction) Act 2006 (Vic) or the Evidence (Document Unavailability) Act 2006 (Vic). However, the knowledge of "looming litigation" would be such a purpose, and the retention of documents in this situation would not amount to a breach of NPP 4.

The Privacy Act does not specifically seek to override specific legal obligations relating to the use or disclosure of personal information.

The Australian Law Reform Commission completed an extensive review of the multi-jurisdiction privacy regime in Australia and submitted its final report to parliament in May 2008. The report was released in August 2008 and relevant recommendations include:

a) The IPPs and NPPs should be consolidated into a set of "Uniform Privacy Principles," or UPPs

b) The Privacy Act and UPPs should apply to the Federal public sector and the private sector – to the exclusion of State and territory laws that deal with personal information and health information

c) The Act's definitions of 'personal information', 'sensitive information' and 'record' should be updated to deal with new technologies and new methods of collecting and storing personal information.

d) The definition of 'record' should be amended to clarify that a record may be stored in electronic or other formats.

e) Organisations should be required to issue data breach notifications to individuals whose personal information has been compromised.

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

The legislation and principles concerning data protection and privacy in Australia (particularly the Privacy Act 1988) and their effect on electronic information is discussed in question 19 above.

The purpose of the Privacy Act is to regulate all aspects of the handling of personal information irrespective of the storage format of the information. The Act regulates the Australian Government, the ACT Government and the private sector.

The Privacy Act itself originated from a period of research in the late 1970s and early 1980s, culminating in a report issued by the Australian Law Reform Commission in 1983. The introduction of the Act dealt with Australia's obligations to implement the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, and Article 17 of the International Covenant on Civil and Political Rights.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The Privacy Act uses the term "personal information" and not "personal data." The Act defines "personal information" as:

> …Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The Act does not provide a definition for the term "processing" (unlike Article 2 of the EU Directive), although it uses the term "electronic data processing" in some specific contexts. Through the NPPs, discussed in question 19 above, the Act imposes obligations at specific points in the handling of personal information (collection, use, disclosure, storage, destruction) and regulates how the information is accessed or corrected by individuals to whom it relates.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

NPP 2 regulates the disclosure of personal information generally, but does not specifically refer to electronic information. It requires that an individual's personal information must only be used (by the collecting party) or disclosed (to a third party) for the primary purpose for which it was collected, unless the use or disclosure (*i.e.*, for a secondary purpose) falls within one of a list of exceptions.

One exception is that the individual has consented expressly or impliedly to the disclosure. A further exception is where the secondary purpose for disclosure is "related" to the primary purpose for which the information was collected. Where the information is "sensitive information," the

secondary purpose must be directly related to the primary purpose for the disclosure to be lawful. Either exception may be applicable to disclosure in legal proceedings or a regulatory enquiry in specific circumstances.

The exception in NPP 2.1 (g), permitting disclosure without the need for consent where it is "required or authorised by or under law" is discussed at question 19 above. Case law has offered little guidance on the necessary extent of "requirement" or "authorisation" before lawful disclosure can take place.

The disclosure of personal information through the production of documents under a subpoena arises from the courts' powers of compulsion and arrest for breach, and (as discussed in question 19) it would fall within this exception. Production for discovery in legal proceedings arises from statute and would similarly fall within the exception. Production to a regulatory enquiry would require the existence of a power of compulsion within its enabling legislation in order to fall within the exception.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

The exceptions discussed in sub-question (c) above do not expressly refer to civil or criminal proceedings.

Some protection is specifically obtained from the rule in *Home Office v. Harman (1983) 1 A.C. 280* that parties to civil litigation are under an implied undertaking to the court to use information obtained through discovery (and other procedures for production in litigation) for the purposes of that proceeding alone.

The rule applies to discovered documents, but also to witness statements filed in accordance with the court's Practice Directions and answers to interrogatories, affidavits, and to documents obtained via subpoena.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

NPP 6 regulates the rights of an individual to access to and the ability to correct personal information held by an organisation about the individual. It does not specifically refer to electronic information.

Under NPP 6.1, as a general principle if an organisation holds personal information about an individual, it must provide the individual with access to the information "on request." Access can be denied or limited in certain circumstances, for example, where the disclosure to that individual would have an unreasonable impact upon the privacy of other individuals.

Another exception exists where the information relates to existing or anticipated legal proceedings between the organisation and the individual making the access request, where the information would not be accessible through discovery in those proceedings.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

These are discussed in question 19 above.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

The Privacy Act and NPPs apply to personal information without reference to the format of the information, and do not regulate electronic information specifically.

As discussed in question 19 above, the Act (and in particular NPP 10) imposes higher levels of protection for the handling of "sensitive information" by private sector organisations. The definition of "sensitive information" includes information about a person's health (including genetic information), racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, sexual orientation or criminal record.

NPP 10.2 and 10.3 permits the collection of health information for providing health services to the individual and for public health research provided the information is de-identified.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

Information about a person's political opinions or membership of a trade union falls within the definition of "sensitive information." The treatment of sensitive information is discussed above.

Private sector employers are exempt from the requirements of the Privacy Act in relation to employee records. This is a point of distinction with the provisions of the EU Directive.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The Privacy Act does not contain notification provisions equivalent to Articles 18 – 21 of the EU Directive.

NPP 1.3 requires an organisation that collects an individual's personal information to take reasonable steps to notify the individual at the time of collection (or as soon as practicable afterwards) of certain matter, including the identity of the organisation, the individual's rights of access, the purpose of collection and the organisations (or types of organisation) to which it usually discloses information of that kind.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

Procedures set out under the Privacy Act for the lawful collection, use and disclosure of personal information (all forms of processing under the EU Directive definition) have been discussed above.

NPP 9 regulates the processing "transborder data flows" out of Australia, but only whilst the personal information is within Australia. It is discussed in greater detail at question 21(a) below.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

As discussed above, employee records in the hands of private sector employers are an exception to the requirements of the Privacy Act.

The Privacy Act does contain provisions requiring consent. These are discussed in greater detail at question 21(a) below.

Cross-Border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Cross-border discovery is possible in limited circumstances other than under the Hague Convention.

Letters of request and letters rogatory are considered by Australian courts. A corresponding procedure arises under section 7 of the Foreign Evidence Act 1984 (Cth), which provides limited means for obtaining documents from outside Australia. Under the Act, and separately from the Hague Convention procedure, an Australian court may issue a "letter of request" to the judicial authorities of a foreign country for the examination of the person on oath or affirmation at any place outside Australia before a judge or officer of the court. A transcript of the evidence may then be provided for submission as evidence in an Australian court.

Domestic procedural rules applied extraterritorially to Australia face the prospect of the Australian blocking statutes discussed at (b) below.

The Privacy Act 1988 regulates transborder data flows of personal information out of the country. The Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) contained in the Act were largely derived from the Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (OECD Guidelines).

NPP 9 contains requirements about when an organisation may transfer personal information about an individual across national borders (hence its title "Transborder Data Flows"). The principle is largely modelled on Articles 25 and 26 of the EU Directive. These requirements currently only apply to private sector organisations. However, the Australian Law Reform Commission is proposing that these requirements should apply to public sector agencies, as well as private sector organisations.

Under NPP 9 an organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country if any one of the following applies:

1) the exporting organisation reasonably believes that the body receiving the information is subject to a law, binding code or contract that imposes similar requirements about handling of information to those in the National Privacy Principles in the Privacy Act; or

2) the individual identified by the information has consented to the transfer; or

3) the transfer is necessary to fulfill a contract with the individual, or for pre-contractual steps requested by the individual; or

4) the transfer is necessary to fulfill a contract that is in the interests of the individual, between the organisation and a third party; or

5) the transfer is for the benefit of the individual, it is impracticable to obtain consent, and the individual would be likely to provide consent if asked; or

6) the organisation has taken reasonable steps to ensure that the information will not be handled in a manner that is inconsistent with the National Privacy Principles.

Where one of these conditions is satisfied, the Australian organisation transferring the data is not liable for subsequent privacy breaches.

Section 13D of the Privacy Act provides that acts and practices required by an applicable foreign law are not considered interferences with the privacy of an individual (and thus potential breaches of the Act) when they take place outside Australia.

In its September 2007 review of the current legislative regime the ALRC criticised the general adequacy of the protection afforded by NPP 9. Its view was that the "reasonable steps" test of NPP 9 provided "little guarantee that personal information will be protected when it is transferred outside Australia. Once an organisation has transferred the information it has lost control over it."

In its May 2008 final report, the ALRC recommended that its proposed model UPPs include a "Cross-Border Data Flows" principle. Under this principle an agency or organisation that transfers personal information about an individual outside Australia would remain accountable for that information, unless:

a) the exporter reasonably believes that the recipient or the information is subject to a law, binding scheme or contract which effectively upholds privacy protections substantially similar to the UPPs;

b) the individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the exporter will no longer be accountable for the individual's personal information once transferred; or

c) the exporter is required or authorised by or under law to transfer the personal information.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

Australia has enacted similar blocking statutes as the United Kingdom.

The initial statutes were the Foreign Proceedings (Prohibition of Certain Evidence) Act 1979 and Foreign Antitrust Judgments (Restriction of Enforcement) Act 1979 as a reaction to the extra-territorial enforcement of US antitrust laws. However, negotiations between the Australian and US governments resulted in the 1982 Antitrust Co-operation Agreement, which provided a framework for notifications and consultation around the US implementation of antitrust laws.

To consolidate the initial statutes, and to give legal effect to its position in the 1982 agreement in the event that it was not followed, Australia enacted the Foreign Proceedings (Excess of Jurisdiction) Act 1984.

Although this explains the historical intent behind the legislation, the powers Australia has enacted are broader in scope. Under the 1984 Act, the Federal Attorney-General may prohibit compliance with foreign discovery orders and judgments in foreign antitrust proceedings if satisfied that the order is desirable "for the protection of the national interest," or where the foreign court asserts jurisdiction which "is contrary to international law or is inconsistent with international comity or international practice."

Amongst other powers, under Section 7 of the Act the Attorney-General may prohibit:

1) the production to a foreign court of documents in Australia;

2) any action in Australia with respect to documents in Australia that might lead to the documents or their contents being produced in a foreign court;

3) an Australian citizen or resident giving evidence in a foreign court about the contents of a document in Australia;

4) the production of documents or the giving of evidence about their contents in an Australian court for the purposes of proceedings in a foreign court.

The authors have been unable to locate any reported cases in which these blocking statutes have been enforced.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The authors have not been able to identify any information in the public domain on this issue.

It should be noted that Section 5B of the Privacy Act protects personal information of an Australian citizen or permanent resident by extending the application of the Act to acts or practices done outside Australia by an organisation.

Bermuda

Paul Smith **- *Lead Editor***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Bermuda is a self-governing, dependent territory of the United Kingdom and part of the British Commonwealth. Bermuda's legal system is a common law system based upon the English legal system. Bermuda has its own legislature which enacts legislation for Bermuda. In addition, however, certain United Kingdom legislation is extended to Bermuda by the UK legislature and takes effect in Bermuda. Bermuda courts frequently cite and apply English case law, and decisions of the English House of Lords and English Court of Appeal are regarded as highly persuasive and are generally followed by Bermuda courts.[22] Decisions of first instance English courts (*i.e.,* the trial courts) and Commonwealth courts are also cited in Bermuda. Their persuasiveness depends on the strength of the judicial reasoning and the standing of the judge who issued the decision. Decisions of the Judicial Committee of the Privy Council are formally binding upon Bermuda courts.[23]

   The legal system of Bermuda is based on the common law. Civil litigation brought in the courts of Bermuda is governed by the rules outlined in the Rules of the Supreme Court 1985 ("RSC") as amended, which are largely based upon the former English Rules of the Supreme Court 1999. Discovery[24] issues are covered by RSC Order 24. Case law has also been used to develop and apply the rules in RSC Order 24.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   There is provision in RSC Order 24 Rule 2 for automatic discovery of documents in actions begun by writ. Actions begun by writ tend to be actions in which there are issues of facts to be determined by the court. There are other forms of originating process in Bermuda (originating summonses, originating motions, and petitions) which do not involve automatic discovery of documents. In the event that the rules providing for automatic discovery are disregarded, the court will make an order for discovery upon the summons for directions. Orders for discovery of documents are sometimes, but not always, made upon the summons for directions in actions begun by originating summons, originating motion or petitions.

   The parties duty to give discovery is the same whether the discovery is automatic or by order of the court. The duty is to give discovery of all documents within the custody, possession or power of the party relevant to the issues in the action, whether or not the documents support its case, adversely affect its case, adversely affect another party's case or support another party's case. A party is required to make a reasonable search for

[22] *See*, *D'Lasala v. D'Lasala* [1979] 2 All ER 1146; *Crockwell v. Haley* [1993] B.D.A. LR 7.

[23] The Judicial Committee of the Privy Council sitting in London is the highest appellate court for Bermuda. The Judicial Committee of the Privy Council acts as the final appellate court for a number of Commonwealth jurisdictions, including Bermuda. The judges of the House of Lords also sit on the Judicial Committee of the Privy Council, thereby ensuring a convergence of judicial reasoning in both the United Kingdom and the Commonwealth.

[24] *i.e.,* Documentary disclosure. There is no oral discovery or deposition procedure in Bermuda.

disclosable documents and the attorneys for a party are under a duty to the court, as officers of the court, to ensure so far as possible that no relevant documents have been omitted from the list of documents.[25]

Upon receipt of a list of documents, the opposing party then has the right to inspect and make copies of any disclosed document, unless the document is no longer in the control of the party who disclosed it, the party disclosing the document has a right or duty to withhold inspection of it on the grounds of privilege, or the court limits the power of inspection.

Automatic discovery takes place 14 days after "close of pleadings" in the action. Discovery by order of the court takes place at the time so ordered. The court will usually set a timetable for disposing of an action at the summons for directions, which will contain provisions for discovery.

The duty of discovery continues throughout the proceedings, and if additional documents come to the party's attention at any time, there is a duty to disclose them.[26]

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

There is no general ability under the RSC or practice in Bermuda to obtain discovery from a non-party. However, (i) the *Norwich Pharmacal* doctrine permits disclosure of documents from a third party in certain limited circumstances and (ii) individual documents known to exist (*i.e.,* documents the existence of which is not conjectural) may be obtained from a non-party under a writ of subpoena *duces tecum*. Writs of subpoena are issued by administrative action of the court under RSC Order 38 Rule 14, and require the person named in the writ to produce the documents specified in the writ. The recipient of a writ of subpoena can apply to set it aside if it requires production of documents in excess of those permitted by law. The limits on the documents which can be obtained by subpoena are laid down by common law: *see*, *e.g., Panayiotou v. Sony Music Entertainment* [1994] Ch 142, and preclude the discovery of classes of documents or indeed anything other than individual documents (not conjectural) which can be separately identified.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The RSC contain no express obligation requiring a party to retain documents.

Until litigation is in reasonable contemplation, there is nothing to prevent an organization from destroying documents in the normal course of business, subject, of course, to its obligations to retain documents for regulatory or statutory purposes.

However, once an order for disclosure has been made, the party must preserve the documents that are ordered to be disclosed. It is a contempt of court intentionally to destroy documents which are the subject of a discovery order (*Alliance & Leicester Building Society v. Gahremani* [1992] 142 N.L.J. 313.)

It is not entirely clear whether there is an obligation not to destroy documents which will be the subject of discovery once proceedings have commenced, but time for disclosure has not yet arrived. In *British American Tobacco Australia Services Limited v. Cowell* (2002) V.S.C.A. 197 the court thought that there was such an obligation, although it did not ultimately matter because the relevant destruction occurred after the time for giving

[25] *Woods v. Martins Bank Ltd.* [1959] 1 Q.B. 55.
[26] *Vernon v. Bosley (2)* [1999] Q.B. 18.

discovery. The court in that case relied upon the dicta of Megarry, J. in *Rockwell Machine Tools v. EP Barrus (Commissionaires) Limited* [1968] 1W.L.R. 693.

However, if there were deliberate destruction of documents after the commencement of proceedings, the Court would not consider this acceptable. In the case of *Infabrics v. Jaytex* [1986] F.S.R. 75, the court applied the maxim "*omnia praesummuntur contra spoliaterem*"[27] against the defendant who had not preserved documents affecting the quantum of damage and had allowed these to be destroyed after the commencement of the action.

Once litigation is in reasonable contemplation, there is still no express rule which prevents document destruction. However, a deliberate decision to destroy relevant documents when proceedings are imminent, or after their contemplation, could involve a criminal offence of obstructing or perverting the course of justice in some circumstances (*R v. Selvage* [1982] Q.B. 372; *R v. Rowell* [1978] 1W.L.R.132), and the Court may also draw adverse inferences from such an exercise.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

A deliberate decision to destroy relevant documents when proceedings are imminent or after their contemplation could involve the criminal offence of obstructing or perverting the course of justice in some circumstances (*R. v. Selvage* [1982] Q.B. 372; *R. v. Rowell* [1978] 1W.L.R. 132). The court may also draw adverse inferences from such an exercise.

Where there has been no compliance with an order for discovery and the lack of disclosure renders it impossible to conduct a fair trial, the court may also consider the remedy of striking out the claim or defence.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

Generally, the court has discretion as to whether costs of an action, or part of it, are payable by one party to another, the amount of those costs and when they are to be paid (RSC Order 62). If the court decides to make an order for costs, the general rule is that the unsuccessful party will be ordered to pay the costs of the successful party, but the court may make a different order (RSC Order 62 Rule 3(3)).

Therefore costs of discovery are treated in the same manner as all other aspects of litigation, that is to say, there is scope for the successful party to recover its costs of discovery from the unsuccessful party. However, the court has discretion to depart from this principle if it deems fit. Factors that will affect this discretion include the conduct of all the parties, whether a party has succeeded on part of his case, even if he has not been wholly successful, and also any payment into court or admissible offer to settle made by a party which is drawn to the court's attention. A failure to disclose documents which are properly disclosable can lead to costs sanctions against the party in default.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

There is no specific guidance in the Bermuda RSC as to how electronic documents are to be dealt with on discovery. There is also very little guidance from the courts as to whether, and to what extent, the parties should carry out a search for electronic documents, although the courts have made it clear that the meaning of

[27] "*Omnia praesummuntur contra spoliaterem*" means "all things presumed against the wrongdoer."

"document" is not restricted to paper writings, but extends to anything upon which evidence or information was recorded in a manner intelligible by the use of equipment, *e.g.,* tape recordings (*Grant v. Southwestern and County Properties Ltd.* [1974] 2 All E.R. 465). The courts had also ruled that a computer database, which forms part of the business records of a company, insofar as it contained information capable of being retrieved and converted into readable form, is a "document" for the purposes of RSC Order 24 and therefore susceptible to discovery (*Derby Co Ltd v. Weldon* (No.9) [1991] 2 All E.R. 901). The word processing file of a computer was also held to be within the definition of a "document" for the purpose of an order preserving documents in connection with proceedings (*Alliance & Leicester Building Society v Ghahremani* [1992] R.V.R 198).

There has been no reported case law in Bermuda dealing with the disclosure of electronic documents or the problems they cause on discovery.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   In Bermuda, under the RSC, discovery is limited to "documents" (RSC Order 24, Rule 1). The RSC do not define "document" but case law establishes that "documents" extends to anything upon which evidence or information was recorded in a manner intelligible by the use of equipment (*Grant v. Southwestern and County Properties Ltd.* [1974] 2 All E.R. 465). The courts have also ruled that a computer database, which forms part of the business records of a company, insofar as it contains information capable of being retrieved and converted into readable form, is a "document" for the purposes of RSC Order 24 and therefore susceptible to discovery (*Derby & Co. Ltd. v. Weldon (No. 9)* [1991] 2 All E.R. 901). The Word Processing file of a computer was also held to be within the definition of a "document" for the purpose of an order preserving documents in connection with proceedings (*Alliance & Leicester Building Society v. Ghahremani* [1992] R.V.R 198).

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

   There are no such specific legal provisions or rules in Bermuda. The Court could, in the exercise of its case management powers under RSC Rule 1A, order the parties to meet and discuss electronic disclosure. It would be necessary for one of the parties to bring the problems of electronic disclosure to the attention of the court in order to persuade the Court to exercise such powers.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

    There are no legal provisions or rules in Bermuda requiring a party to preserve electronic documents related to pending or possible future litigation. See, however, the general provisions about retention of paper documents above, which would also apply to electronic documents.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

    There are no such legal provisions or rules in Bermuda. However, the general provisions about searching for discovery and providing paper documents set out above would apply to electronic documents.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

    There are no such legal provisions or rules in Bermuda.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

    There are no such legal provisions or rules in Bermuda. The general provisions about production of paper documents set out above would apply to electronic documents.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

    There are no such legal provisions in Bermuda. It would be necessary for the parties to apply to court for a determination of such matters on an ad-hoc basis. The Bermuda court has power under RSC Order 24 Rule 8 to limit discovery where it considers the discovery is "not necessary either for disposing fairly of the cause or matter or for saving costs."

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

    Privileged documents mistakenly disclosed can generally be used by the receiving party on the basis that they are no longer the subject of legal professional privilege where it was not obvious to a reasonable attorney that a mistake had been made in disclosing them, subject always to the court's powers of case management (*see*, *Al Fayed and Others v. Commissioner of Police of the Metropolis* [2002] E.C.W.A. Civ. 780).

    Where it is obvious to a reasonable attorney that a mistake has been made in disclosing privileged documents, it may be possible to obtain injunction requiring the privileged documents to be retained by the recipient and to prevent use of the information contained in them: *see*, *Derby & Co. Ltd. v. Weldon (No. 8)* [1991] 1 W.L.R. 73.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

    There are no specific rules dealing with costs of electronic discovery. Costs of this type of disclosure therefore follow the same principles as costs in relation to the rest of the discovery process as found in RSC Order 62 (see question 6 above). It is to be remembered that the court has complete discretion as to when and in whose favour costs are to be awarded.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

    There are no legal requirements in Bermuda for the adoption of information management policies and procedures. As a matter of practice, the larger businesses in Bermuda do adopt their own information management policies and procedures.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

    There are no legal requirements in Bermuda for the adoption of information management policies and procedures. As a matter of practice, the larger businesses in Bermuda do adopt their own information management policies and procedures.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    Bermuda has no specific privacy or data protection legislation. In Section 26 of the Electronic Transactions Act 1999 there is power to make regulations prescribing standards for the processing of personal data, but no such regulations have been made. The government has, however, announced that data protection legislation is in preparation.

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

    a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

    b. *The legal definition of "personal data" and "processing" of data within your jurisdiction.*

    c. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    d. *Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.*

    e. *Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.*

    f. *Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.*

    g. *Any specific data types, subject areas or situations for which electronic discovery is restricted.*

    h. *Any employee, employer, union or other contractual considerations related to electronic data and discovery.*

    i. *A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.*

    j. *A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.*

    k. *Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)*

    Bermuda has no specific privacy or data protection legislation. In Section 26 of the Electronic Transactions Act 1999 there is power to make regulations prescribing standards for the processing of personal data, but no such regulations have been made. The government has, however, announced that data protection legislation is in preparation.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

Bermuda is not party to the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters. However, under Part IIC of the Evidence Act 1905, Bermuda courts give effect to in-coming Letters of Request from foreign courts for evidence required for trial of foreign litigation, broadly as if the Hague Convention were applicable in Bermuda. This is however subject to the same reservation as expressed by the United Kingdom when it adhered to the Hague Convention, namely that its provisions are not to be used to conduct discovery exercises.

The Letter of Request process under Part IIC of the Evidence Act 1905 is the exclusive method of obtaining evidence by compulsion in Bermuda for use in foreign courts.

This process is subject to the following limitations, as established by statute and at common law:

a. Discovery of classes or categories of documents is not permissible.

b. Disclosure of conjectural documents is not permissible.

c. The documents sought must be evidence required for trial of the foreign litigation and must be separately identified in the Letter of Request. It is permissible to request batches of documents but only if the documents can be separately identified as actual and existing documents.

See generally Panayiotou v Sony Music Entertainment [1994] Ch 142 and *Netbank v. Commercial Money Center* [2004] Bda L.R. 46.

There is no blocking statute in Bermuda.

Brazil

Altamiro Boscoli - ***Lead Editor***
Thomas Belitz Franca - ***Contributing Editors***
Renato Opice Blum, Juliana Abrusio - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Brazil is a civil law jurisdiction. Its judicial system relies heavily on legislation passed by the Legislative (Federal Congress). Federal law governs most substantive areas of the law, although it can be supplemented by various laws of states and municipalities.[28] The traditional role of the courts is to interpret statutes and contracts in light of particular facts. Case law is not binding, and is just one source of persuasive legal authority[29] in the Brazilian system. Judges often look to the equities of a case and the general practice of the community as guidelines for deciding a case.

   Although the Brazilian law does not provide for the concepts of *stare decisis* and dicta, dissenting opinions can be used as persuasive arguments by the parties, mainly when these opinions were issued by higher courts and supported by a formal court precedent. Another distinctive aspect of Brazilian law that would probably call the attention of a common law practitioner is the judicial tendency to rely on reputable scholars to ground decisions. Legal doctrine is an important tool in litigation in Brazil. It is rather common for lawyers to quote works from renowned scholars, judges or reputable attorneys. These opinions, together with case law, usually serve as a strong persuasive argument.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   In civil court proceedings, the judge may order that the party should disclose evidence or anything that may be in the party's possession, provided that the adversary party shows the need and convenience for the disclosure requested. However, the party may refuse, provided that such refusal is justifiable, to disclose the requested document, whereas the judge will not admit such refusal where (i) the demanded party is legally required to disclose; (ii) the demanded party alluded to the document or the thing in the proceeding for the purposes of adducing evidence, and (iii) the document, given its content, is common to both parties.

   The judicial disclosure of account books and documents kept on the files of the company may be required in three situations: (i) the company's liquidation; (ii) succession due death of a partner, and (iii) by specific legal order.

   Finally, the judicial disclosure of documents is possible in the cases the document is proper or common, is in possession of a co-interested party, partner, co-owner, creditor or debtor; or in possession of a third party that

[28] Contracts, family, consumer and torts law, corporate and securities laws, antitrust, federal taxes, administrative law, procedural law, insurance and reinsurance and so forth. A good side effect of having many bodies of law regulated by federal laws is that conflicts of law become a fairly simple subject.
[29] Introductory Law to the Civil Code lists (hierarchically) the sources of law: legislation, case law, general principles of law, analogy, custom and usage, equity and legal doctrine.

is their custodian in the capacity of administrator of a estate, executor, depositary or administrator of others' properties.

The nature of the disclosure of documents is that of the obligation to do.

The disclosure of documents, as a rule, occurs at the probative stage (all pieces of evidence are produced in the proceeding at a stage that we call "probative"). However, it may also be required through a provisional remedy in preparation for the suit, to "constitute or ensure evidence, or, in some cases, for the exercise of a simple right to know or examine the object in possession of a third party,"[30] as well as incidental to the principal action. Finally, there is the independent proceeding for disclosure whose main protection purpose is exactly protecting the party's material right to the disclosure of the document and which ends upon the fulfillment of the determination.

In civil court proceedings, the burden of proof is put on the parties: on the requesting party, to prove the facts that compose its right, and on the requested party, to prove the facts that extinguish, modify or curb the right of the other party. Thus, the disclosure must be requested by the party or determined ex-officio by the judge and never is it an automatic obligation.

After the disclosure of the document and after the purpose of its disclosure is fulfilled, the document is returned to the party that disclosed it, unless the judge orders otherwise.

The procedures are described in the Code of Civil Procedure:

Section IV

Disclosure of Document or Thing

Art. 355. The judge may order that the party disclose a document or thing that is in the party's possession.

Art. 356. The request made by a party shall contain:

I – the identification as complete as possible of the document or thing;

II – the purpose of the proof, indicating the facts related to the document or thing;

III – the circumstance grounding the requested party's assertion that the document or thing exists and is in possession of the adversary party.

Art. 357. The requested party shall answer within 5 (five) days subsequent to the legal notice date. Should the party state that it does not have the document or thing, the judge will authorize the requesting party to prove through any means that that statement is not true.

Art. 358. The judge will not admit a refusal:

I – if the requested party has a legal obligation to disclose;

II – if the requested party alluded to the document or thing in the proceeding with the purpose of constituting evidence;

III – if the document, given its content, is common to the parties.

[30] THEODORO JÚNIOR, Humberto. *Processo Cautelar*. 22nd rev. and current edition. São Paulo: Liv. e Ed. Universitária de Direito, 2005, p. 296.

Art. 359. When deciding on the request, the judge will admit as true the facts that, by way of the document or the thing, the party intends to prove:

I – if the requested party does not disclose it or does not make any statement within the term referred to in art. 357;

II – if the refusal is considered unlawful.

Art. 381. Upon request by the party, the judge may order the full disclosure of the account books and documents kept on the files:

I – in the case of liquidation of the company;

II – in the case of succession due to death of a partner;

III – where and how the disclosure is determined in law.

Art. 382. The judge may order ex-officio the party to disclose a part of the books and documents, by extracting from them the essence that is relevant to the litigation, as well as making certified copies of it.

Section V

Disclosure

Art. 844. As a preparatory procedure, there will be the disclosure of:

. . .

II – proper or common documents in possession of a co-interested party, partner, co-owner, creditor or debtor, or in possession of a third party that is its custodian in the capacity of administrator of a estate, executor, depositary or administrator of others' properties;

III – full account books, balance sheets and documents kept on the company's files, in the cases expressly provided for in law.

Art. 845. As to the procedure, the provisions in arts. 355 through 363, and 381 and 382 shall be observed, as applicable.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

The same procedure followed to compel a party to disclose documents may be applied to a third party aiming at such purpose. In the case of a third party, this third party is served notice to state that it will or will not disclose the document, and the third party's refusal shall be admitted (i) if it concerns to business of the life of that third party's family; (ii) if its disclosure may violate a duty of honor; (iii) if making the document public will cause loss of honor for the party or the third party, as well its relatives by blood or up within third-degree relatives of the party; or if the disclosure represents risk of criminal action; (iv) if the disclosure causes dissemination of fact, which due to status or profession, must be kept secret or (v) if there are serious reasons, which, upon prudent decision by the judge, justify the refusal to disclose.

The nature of the measure is that of the obligation to do, and a writ of seizure and request for police reinforcement may be issued if after the third party has been heard and the disclosure of the document determined, the order is not obeyed within five days.

Likewise, the procedures are described in the Code of Civil Procedure:

> Art. 360. Where the document or thing is in possession of a third party, the judge will order that said third party be summoned to provide answer within ten (10) days.
>
> Art. 361. If the third party denies the obligation to disclose or the possession of the document or thing, the judge will schedule a special hearing to take deposition from the third party as well as from the parties and, if need be, from the witnesses; following, the judge will pass judgment.
>
> Art. 362. If the third party, without fair reason, refuses to disclose, the judge will command the third party to deposit the document or thing in the court of records or at any other designated place, within five (5) days, and will order the requesting party to reimburse the third party for the expenses; if the third party disobeys the order, the judge will issue a writ of seizure, and if necessary, will demand police reinforcement, all without prejudice to the liability for crime of disobedience.
>
> Art. 363. The party and third party that are excused from disclosing in court a document or thing:
>
> I – if it concerns to business of the own life of the family;
>
> II – if its disclosure may violate a duty of honor;
>
> III – if making the document public will cause loss of honor for the party or the third party, as well as its relatives by blood or up within the third degree; or if the disclosure represents risk of criminal action;
>
> IV – if the disclosure causes dissemination of a fact, due to status or profession, it must be kept secret;
>
> V – if there are serious reasons, which, upon prudent decision by the judge, justify the refusal to disclose.
>
> Sole paragraph. If the reasons referred to in I to V concerns only a part of the content of the document, the essence of the other part will be extracted to be presented in court.
>
> Art. 844. As a preparatory procedure, there will be the judicial disclosure:
>
> I – of the movable thing in possession of others and that the requesting party considers of its own or is interested in knowing; . . .

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The documents must be preserved by the parties for the purposes of evidence, at least during the statute of limitations period, namely:

A) During an internal investigation or before a judicial or an arbitration process:

1. Consumer claims:

Documents:

- internal reports related to the products
- recall reports
- customers claims
- letters to customers
- transactions or agreements with customers
- payment receipts
- electronic documents

Time-barred:

- 30 days to claim apparent or easily-detectable defects in regard to supply or services and non-durable products
- 90 days to claim apparent or easily-detectable defects in regard to the supply or services and non-durable products
- 5 years to claim damages caused by a product or service

2. Damage claims not involving consumer rights:

Documents:

- internal reports
- notification, claims and replies
- transactions or agreements
- payment receipts
- electronic documents

Time-barred:

- 1 year to claim damages for loss of or damage to goods carried by railroad
- 3 years to claim civil relief, recovery for unlawful enrichment and loss of profits or dividends received in bad faith

3. Collection claims:

Documents:

- letters of credit, promissory notes, trade bills and checks
- agreements or contracts related to the debt
- payment notice
- protest of bill
- transactions or agreements
- payment receipts
- electronic documents

Time-barred:

- 1 year to file action related to negotiable instrument against the endorser and respective guarantor
- 6 months to receive check payment
- 3 years to receive payment of instrument of credit, especially trade bills, as of the due date
- 5 years to execute promissory note, and bill of lading against the drawer, beneficiary and respective guarantors

4. Contract law claims:

Documents:

- enforcement of contracts and execution of receipts of payment related to such contracts
- addendum to the contracts
- mail exchange between the parties to the contract related to the essential elements of the contracts
- electronic documents

Time-barred:

- 5 years for collect claims related to the contracts
- 10 years for any other claim related to the contracts

B) During a judicial or an arbitration process:

Documents

- complaint
- defense

- transcription of hearings
- award and appellate decision
- certificate of res judicata
- electronic documents

Time-barred:

- during the entire process

C) After a judicial or an arbitration process:

Documents

- award and appellate decision
- certificate of res judicata

Time-barred:

- 90 days to file action for annulment of arbitration award
- 2 years to file action for annulment of trial court judgment or appellate court decision
- 5 years for collection claims based on a judicial or arbitration award
- 10 years after the final decision rendered in the proceeding for all other claims

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

If the party has any documents that such party is required to disclose, the facts that should be proved by the adversary party through the disclosure of said documents are presumed true. With respect to the third party, if the punitive order is made, the writ of search and seizure regarding the document will be applicable, without prejudice to the accusation of crime (disobedience).

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

The costs in civil proceedings are always borne by the defeated party. If the party requested, and the court granted, disclosure of documents, the costs and expenses are borne by the adversary party. In case a third party is commanded to disclose, the party that demanded such evidence will advance the costs and expenses, and eventually, they will be reimbursed by the defeated party.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

In general, one can say that the Law does not follow the social, economic and technological developments, and usually falls behind other social evolutionary developments. The lack of regulation on e-documents, so that

their legal validity is yet to be acknowledged, is nowadays one of the major obstacles to the development of electronic proceedings, but even so we have been verifying that several rules have been added to our legal system to validate such documents.

Electronic proceedings in Brazil are regulated by Law 11.419/2006, which specifically provides for the performance of procedural acts, such as filing of petitions and appeals and rendering of decisions via the Internet. It should also be mentioned Provisional Measure no. 2.200/2001, which introduced the legislative competence on the issue in Brazil by creating the ICP-Brazil and dealing with the issue of safety and legal validity of e-commerce and e-documents. It is important to note that though Provisional Measures are named "provisional" they are in full force and are equivalent to any other laws.

The Brazilian Civil Code considers photographic reproductions, cinematographic, photographic registers and in general any other mechanic or electronic reproductions of facts or things as full evidences, if not rejected by the other party.

The Civil Procedure Code also has similar provisions on article 383, that are compatible with a more liberal theory, adopted by the Brazilian Civil Code in its Article 107 regarding the freedom of the form of the declarations in general ("The validity of the declaration of intentions do not depend on a special form, except when set expressly forth by the law"). As we pointed out above, the use of analogy is also important in the Brazilian jurisdiction.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

First we should clarify that the concept of "disclosure," as it exists in the American legal system, has no correspondent in the Brazilian system. Here, all pieces of evidence are produced in the proceeding at a stage that we call "probative," as already mentioned. Such stage begins upon the parties' presentation of documents, which usually are attached to their first statement. Further, the expert evidence is produced, and after that, the testimonial evidence. All such pieces of evidence are submitted to a judge, who coordinates their submission.

We stress that there is no legal definition of "electronic document," and the following definition is customarily accepted: the digital document, named electronic document or "computing" document is any document produced by using a computer or other digital system.

Concerning crimes against immaterial property, the Brazilian Criminal Procedure Code in its Article 529 sets forth that a previous expert report is necessary. Also, when the infraction leaves vestiges, a body of offense examination must be collected, according to the provisions of Article 158 of the Brazilian Criminal Code.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

As mentioned, the Brazilian legal system has no "disclosure stage" as the American system has, so that all proofs are attached to the case record during the probative stage.

In this fashion, the provisions in the Code of Civil Procedure, including provisions on electronic proceedings, prescribe mechanisms and terms for the parties to present documents and make statements, however, the parties hold no prior discussion on them.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

Article 11 of Law no. 11.419/2006 determines that documents that are electronically produced and attached to electronic proceedings with guarantee of provenance and addressee are considered legal for all purposes. And paragraph 3 of the same article specifies that not the digitalized documents, but rather their originals, must be preserved:

> The originals of digitalized documents . . . shall be preserved by the party that holds them until the judgment becomes res judicata, or where admitted, until the end of the term for filing a rescissory action (seeking annulment of the judgment).

One may say that, under a rule of the Brazilian Civil Law, the electronic documents must be in the custody of their holders during the respective statute of limitations period or laches period, as indicated in question 4 above.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

According to Law no. 11.419/2006, in case the electronic means is admitted in the development of judicial proceedings, communication of acts and transmission of procedural documents, these should be made remotely, preferably by using the computers' world network.

Furthermore, the electronic signature will be the unequivocal form to identify the signatory, and its prior certification at the Judiciary Branch is compulsory, as well as the identification upon presence must be based on a digital certificate to be issued by the Accredited Certifying Authority [Autoridade Certificadora Credenciada] (for instance, Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brazil). Otherwise, the electronic document will not be admitted and acknowledged as valid in a proceeding in course in the Judiciary Branch.

Regarding electronic proofs, including electronic documents, the possibility of their existence was acknowledged by article 225 of the Civil Code in effect, and this promotes the electronic proceedings with digital certification, under Provisional Measure no. 2.200-2/01: "Article 225 – The photographic and cinematographic reproductions and the phonographic recordings, and, in general, any other mechanical or electronic reproductions of facts and things are full proof of them, if the party against which they are presented, does not challenge their correctness."

There are Bills of Law in progress (PLS 76/2000, PLS 137/2000, and PLC 89/2003) regarding electronic crimes that set forth standards of responsible for providing access to a computer network that would keep records in a controlled and safe environment for the period of 3 (three) years, to protect data and any other information requested by investigations upon a judicial order and to disclose information to the competent authorities in cases of criminal suit.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

Up to this date, there are no legal provisions or rules in Brazil (in place or proposed) that require a party to verify whether a search for electronic documents has been carried out. What we have in Brazil are the provisions of the Civil Procedure Code and Criminal Procedure Code regarding search and seizure and previous production of evidence. Other provisions can be found in Law 9296/96, which considers it criminal to

intercept the telematic flux (to intercept telephone, informatics or telematic communications or to disrupt secret of Justice without judicial authorization).

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

The form of producing documents in judicial proceedings is regulated by Law 11.419/2006. Specifically, Article 11 of said law, which, as mentioned, determines that, for all purposes, the documents electronically produced and attached to electronic proceedings are fully effective, also provides that:

(i) digital statements and digitalized documents attached to the record by the Legal Courts and their instrumentalities, by the Department of Justice and its instrumentalities, by the Attorney's Offices, by the police authorities, by the public agencies in general, and by public and private attorneys have the same proving power as the original ones, save in case of justifiable and grounded allegation of falsification occurred before or during the digitalization process (paragraph 1);

(ii) where the digitalization of documents is technically unfeasible due to a great number of documents or due to illegibility, such documents must be presented to the court of records or the court administration office within ten (10) days as of the date the electronic petition informing on the fact is sent, and such documents will be returned to the party after the judgment has become res judicata (paragraph 5);

(iii) the digitalized documents attached to an electronic proceeding will be made available to be accessed by the parties to the proceeding and by the Department of Justice only via the external network, subject to the legal provisions on confidential events and in camera proceedings (paragraph 6).

MP 2200 has provisions on the producing of electronic evidences, as long as the form they may be produced. The Civil Code Article 225 also contains provisions regarding the liberty of form of evidences when not set forth by the law.

Another standard is ISO 17799/2005, which sets forth rules on information security and is valid in Brazil, not as a law, but it serves as a technical standard which is observed.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

According to Law no. 11.419/2006, the electronic proceeding will be as effective as those that follow the ordinary course, *i.e.*, all petitions, appeals and other documents that the authorized parties deem necessary may be attached to the electronic proceeding, and no filtering system will prevent their inclusion in the record (unless in the event of full contravention of the procedural laws).

Thus, all acts produced in the electronic proceedings are fully effective for all legal purposes, however they must contain electronic signature as provided for in law, and will be accessible only to the parties to the proceeding and the Department of Justice. It should be noted that an allegation of falsification may also be submitted electronically.

It is important to note the provisions contained in Provisional Measure 2200/2001, which created ICP-Brazil (digital signatures) and also deals with issues like safety and legal validity of electronic documents. When said electronic certificate provided by ICP-Brazil is applied there is the presumption of validity and authenticity.

Other important means of providing evidence are: (i) through a notary public record, *i.e.,* a notary public, who has authority to attest documents, declares the authenticity of an electronic document; (ii) expert evidences generated by expert reports; and (iii) injunction measures.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

Law no. 11.419/2006 provides that the records of electronic proceedings must be protected by systems for access safety, and the same protection must be afforded to the authorized parties, the digitalized documents and all other procedural acts.

However, said Law does not set forth the penalties to be imposed on those that may violate the confidentiality and/or the secrecy of such information, so that violators will be imposed the penalties set forth in the Brazilian civil and criminal laws.

The 11767/08 Law sets forth provisions on the inviolability of law firms and lawyers' workplace as to the information regarding their law services. Written, electronic, telephonic and telematic correspondences are protected, as long as they are related to the exercise of lawyering.

The Brazilian Criminal Code sets forth penalties for those who, without just cause, reveal secret information obtained upon the exercise of profession or by any means facilitates the access to such information, in Articles 154. In Article 325, there are specific provisions for employees of the public administration when violating confidential information.

There are Bills of Law (PLS 76/2000, PLS 137/2000, and PLC 89/2003) that address crimes using electronic means, suggesting the broadening of Article 154 dispositions, including the disclosing, utilizing, commercializing of providing personal data and personal information contained in computer systems and other penalties.

The Industrial Property Law, in its Article 195, IX, XII and XV sets forth sanctions for the disclosing of sensitive information (commercial or industrial knowledge, information, confidential data) by employees or obtained by illicit means, with penalties of detention from 3 months up to 1 year, or fines.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

Law no. 11.419/2006 does not lay down rules on difference in costs to file an action (or any other filing related to a proceeding), where such action follows the electronic course.

However, Article 13 of said law provides that the judge may determine that the electronic via to be used to produce and send data and documents necessary to support the proceeding, and such procedure may be performed through any available technological means, *preferably* incurring less costs, considering its efficiency.

As mentioned above in question 6, the costs of electronic disclosure are always borne by the defeated party in a process. The party that demanded such evidence will advance costs and expenses, which will eventually be reimbursed by the defeated party.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

Law no. 11.419/2006 determines that, in the first place, the party authorized by the Judiciary Branch that will send petitions, appeals and perform all other procedural acts via the electronic means be provided with registration and means to access the system so as to preserve the confidentiality, identification and authenticity of the communications.

Further, Article 11 of said law also provides that all digitalized documents attached to electronic proceedings will be available for access only to the parties to the proceeding and the Department of Justice, subject to the legal provisions on the events of confidentiality and in camera proceedings.

Finally, Article 12 provides that the records of electronic proceedings must be protected through access safety systems and stored in a means that ensures the preservation and integrity of the data and dispenses with the creation of supplementary records.

The records retention schedules must be kept for the statute of limitations length of time, as mentioned above. Regarding business, especially on the internet, policies such as websites´ terms of use may serve as evidence in a judicial process to indicate a possible bad faith of the user. Internal policies of use adopted by companies for the use of its informatics systems may serve as evidence in a judicial process as well, indicating possible bad faith of the user.

As mentioned above, another important standard is the ISO 17799/2005, regarding information security.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

As already mentioned, the Law does not follow the social evolutionary developments, but rather, in general, it responds to them. Even though, in Brazil the information technology has been expanding to reach the most different areas and experiencing a rapid development including in the judicial system.

In view of the increasing number of professionals that work in the area and the fact that several sectors use the information technology to sign, file and organize documents, further to the already existing Law (11.419/2006) and the ongoing bills, there is a trend towards the introduction of other rules and regulations to perfect our judicial system and define the electronic course of the judicial proceedings.

The Brazilian laws already recognize the validity and authenticity of electronic documents according to Provisional Measure 2200/2001, as mentioned above.

As mentioned above, the Brazilian Civil Code (Art. 225) and Civil Procedure Code (Article 383) also are favorable to the using of electronic documents, when the law does not set forth differently.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

Pursuant to the Brazilian constitutional principles, the rules and regulations established in other jurisdictions are accepted by our legal system only in very exceptional cases (international treaties, for example). The Brazilian Constitution, as well as the Brazilian Civil Code and Code of Civil Procedure, among others, lay down detailed rules on in camera proceedings, privacy and confidentiality concerning production, use and safeguard of documents.

Initially, Article 5, item XII, of our Federal Constitution provides that the confidentiality of mail and telegraphic communications, telephone data and communications, save, in the last case, upon a judicial order, is inviolable.

The Code of Civil Procedure determines that the procedural acts shall be public; however a proceeding will be heard in camera where the public interest so demands as well as those related to marriage, parenthood, separation of spouses and its conversion into divorce, alimony and custody of child. It also provides that the right to examine acts and apply for certificates is restricted to the parties and their attorneys in fact.

The Ethics Code of the Brazilian Bar Association also regulates the secrecy, as it is inherent in the law practice, and the attorney must keep secret any information obtained by reason of the practice and will refuse to testify in proceedings that are or were in his/her care or against a person for whom he/she is acting or has acted.

Accordingly, in regard to the cases in which the secrecy is imposed by law, we understand that the electronic documents and their production in court must obey the privacy rules as indicated above.

The Federal Constitution also sets forth that the rights of intimacy, privacy, honor and image are inviolable in its Article 5, X.

Similar rules are foreseen by Brazilian Civil Code it its Articles 20, when it comes to non authorized divulging, publishing or using of the image of natural persons. Article 21 sets forth rules on the inviolability of the privacy of natural persons.

Regarding the privacy of personal data, the Brazilian Consumer Code sets forth rules on the records of personal data and information of the consumer, which must always be communicated to the consumer. Also, the consumer has the right to have access to all his or her information recorded.

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

As a general rule, the Brazilian legislation prescribes the protection of any form of communication between natural persons, which is guaranteed under both the Federal Constitution and the ordinary laws that govern individual rights to privacy, information confidentiality and private life.

Article 5, item X of the 1988 Federal Constitution protects the privacy and private life of natural persons, guaranteeing their right to be compensated for pecuniary damages or pain and suffering caused by any violation of said right.

Item XII of that same Article 5 provides in a more detailed fashion for the inviolability of the confidentiality of mail and telegraphic communications, and data and information communications. In the last case, the confidentiality may be violated only upon judicial order, in the events set forth and as provided for in law, for the purposes of criminal investigations or supporting criminal proceedings.

The confidentiality of personal communications may be suspended in the event of state of siege or defense, as provided for in the Federal Constitution, Article 136, § 1, items "b" and "c," in which events the personal interest of the protection cedes to the social interest of security.

On the other hand, Articles 151 and 152 of the Brazilian Criminal Code, in accordance with the constitutional provisions, establish punishments for anyone that unduly tampers with a closed mail addressed to another person as well as anyone that unduly takes possession of other's mail, in whole or in part, or withholds or destroys it. The penalties will be heftier if the person trespasses on his capacity as partner or employee of a company and performs any of such acts as regards commercial mail.

The uncodified legislation specifically provides for electronic documents, under Federal Law no. 9296/96. Article 10 of said Law sets forth that intercepting computing information, where not judicially authorized, is a crime.

There are Bills of Law (PLS 76/2000, PLS 137/2000, and PLC 89/2003) that address crimes using electronic means that sets forth that providers must store data and information for the period of time of at least 3 (three) years.

Similar rules are foreseen by Brazilian Civil Code it its Articles 20, when it comes to non authorized divulging, publishing or using of the image of natural persons. Article 21 sets forth rules on the inviolability of the privacy of natural persons.

Regarding the privacy of personal data, the Brazilian Consumer Code sets forth rules on the records of personal data and information of the consumer, which must always be communicated to the consumer. Also, the consumer has the right to have access of all his or her information recorded.

The Brazilian Criminal Code sets forth penalties for those who, without just cause, reveal secret information obtained upon the exercise of profession or by any means facilitates the access to such information, in Articles 154. In Article 325, there are specific provisions for employees of the public administration when violating confidential information.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The Brazilian legislation does not contain an express legal definition of personal data or processing of data, so that the legal definition of such terms remains up to the doctrine and the case law.

Personal data may be described as elements of information or representation of facts related to a person, in a proper form of storage, processing or transmission through automatic means.

Processing of data consists in analysis of the content of the data in question and the relations obtained through such analysis.

Data protection may be understood as protection of information restricted to ordinary access. They are, therefore, data considered private and of relevant interest of either a natural person or a legal entity.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

See answer to question 19 (excluding the last three paragraphs thereof). Also, see answer to question 15.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

They apply to both proceedings.

As provided for in the Federal Constitution, the protection of personal data and information is limited by a request for confidentiality breach for the purposes of criminal investigation and supporting criminal proceedings.

In addition to guaranteeing the fundamental rights to privacy and private life of natural persons, the Federal Constitution introduced the "habeas data," an action that permits the interested party to access the party's personal information recorded in any database as well as to correct them.

The Civil Code prescribes that non-authorized disclosure of information and violation of the right to privacy are subject to compensation for pecuniary damages and pain and suffering, and a provisional remedy preventing any violation or ordering that any violation ceases.

The Consumer Protection Code establishes that the consumer must be informed in writing of any gathering of the consumer's personal information for registers or record files, where not requested by the consumer. The consumer is ensured access to any information about the consumer, either personal or business information, and may correct or update such data.

The Consumer Protection Code further establishes that refusing the consumer access to his/her personal data and failure to update such data where they are knowingly incorrect constitute a crime.

In regard to violation of mail and communications, the Criminal Code establishes that an employee commits a crime when he/she takes advantage of his/her position as employee to divert or hide the employer's mail and disclose the employer's secrets, among other events.

The banking legislation provides for the confidentiality of banking operations and banking services and establishes that breach of that confidentiality is a crime. However, it lists some events that do not constitute violation of the duty of confidentiality, such as information exchange between financial institutions, supply of information to credit protection entities and communication of unlawful acts to the authorities.

Also, see answer to question 15.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Article 5, items X and XII, of the Federal Constitution guarantees the protection of natural persons' private life, privacy, honor and image and draws a clear limit to the right to information. It further guarantees the inviolability of communications of thought that do not aim at indeterminate public as well as the confidentiality of data.

Under the Brazilian legislation, the legal persons are expressly ensured protection of the corporate entity and industrial property. The entity, the element that makes a person, either natural or legal, holder of rights and obligations, an effective participant in the legal system, both independent and liable for such person's acts, is under the aegis of the Brazilian Civil Code, Articles 11 through 21. As expressly mentioned in Article 52 of that Code, the protection of the rights applies to legal persons, as applicable. As to industrial property, Article 2 and corresponding items of Law no. 9.279/1996 provide for the protection of rights related to industrial protection.

With respect to legal persons, there is also the possibility of a contractual clause providing for the confidentiality of information arising from the commercial relationship between the parties to an agreement and expressly stipulating the applicable penalties in case of nonperformance.

Finally, it should be mentioned that any misuse of information negatively affecting a natural or legal person may constitute crime against the honor, as, for example, defamation.

There are no specific laws regulating privacy as set forth in the Constitution. The Bills of Law in progress mentioned above foresee crimes utilizing electronic, digital or similar systems and contain rules on forgery of electronic data or private documents, undue disclosing or misuse of information and personal data, obtaining, transporting or providing data or information without authorization, among others.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

The rules established to protect the privacy and confidentiality of data are effective in the federal sphere and any exception will be authorized only upon judicial order and to the benefit of a criminal investigation or in support of a criminal proceeding.

The request for breach of confidentiality must be duly justified, evidencing that the information protected by law is indispensable for the investigation development.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

There is no restriction as to the evidencing ability of electronic documents. The possibility of its existence was acknowledged in Article 225 of the Civil Code in effect: "Article 225 – Photographic and cinematographic reproductions, phonographic recordings and, in general, any other mechanical or electronic reproductions of facts or things evidence them in full, if the party against which they are presented do not object to their correctness."

There are restrictions, though, when it comes to the duty of confidentiality of certain professionals as lawyers. A recent law passed (Law 11.767/2008) recognizing the inviolability of law firms and lawyers' workplace as to the information regarding their law services. Also, written, electronic, telephonic and telematic correspondence are inviolable, as long as related to the exercise of lawyering.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

The electronic mail or e-mail given by the company to the employee (corporate email) is not equivalent to regular mail and private phone calls, and is not afforded the constitutional protection of privacy and inviolability. The exercise of the employer's right to property is guaranteed through a formal control (quantity, addressee, etc.) or material control (content control) of the electronic mail.

As the employer supplies its employees with the tool, for the sole purpose of enhancing the development of their activities, the data stored as a result of the corporate e-mail tool is the employer's property. This is a widely accepted understanding both in the labor and the criminal spheres.

To avoid questioning on privacy prerogative by the employees, we strongly recommend the companies to adopt a "Policy for Use of Computing Property," describing the employees' obligations as to the handling of the corporate e-mail, as well as establishing rules for the company's monitoring.

Another important contractual consideration is the one concerning non-disclosure agreements commonly used in employment relations.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The right of communication plays a central role in the globalized scenario in which Brazil is included, whereas the individual rights like data privacy and confidentiality are considered fundamental rights.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

A judicial authorization is required to obtain personal data of either natural or legal persons, in the events set forth in law, aiming at a criminal investigation or supporting a criminal proceeding.

Obtaining such data without a judicial authorization constitutes crime, punishable by penalty of imprisonment of three months to one year, and a fine.

The breach of the confidentiality of personal data may be claimed by any authority involved in the criminal investigation or in fact-finding in criminal proceedings, namely, the Chief Police Officer, the Department of Justice or even the judge.

The legislation that regulates the breach of confidentiality of banking data is Supplementary Law no. 105/2001 and that regulates the breach of confidentiality of telephone data is Federal Law no. 9296/96.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

In Brazil, there is a consensus about the importance of the issue of personal data processing at the workplace. In fact, a great number of routine activities performed during the employment relationship results in the gathering of personal data of employees.

To select, train and promote workers, as well as to control the quality and increase the production, in addition to other countless purposes, the companies regularly process their employees' data.

Such data, however, are considered private and the companies have no legal authorization to disclose/market them, under pain of being held liable, except where they obtain the acknowledgment and consent in writing from each employee.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

Brazil is a civil law jurisdiction. Its judicial system relies heavily on legislation passed by the Legislative (Federal Congress). Federal law governs most substantive areas of the law, although it

can be supplemented by various laws of states and municipalities.[31] The traditional role of the courts is to interpret statutes and contracts in light of particular facts. Case law is not binding, and is just one source of persuasive legal authority[32] in the Brazilian system. Judges often look to the equities of a case and the general practice of the community as guidelines for deciding a case.

Although Brazilian law does not provide for the concepts of *stare decisis* and dicta, dissenting opinions can be used as persuasive arguments by the parties, mainly when these opinions were issued by higher courts and supported by a formal court precedent. Another distinctive aspect of Brazilian law that would probably call the attention of a common law practitioner is the judicial tendency to rely on reputable scholars to ground decisions. Legal doctrine is an important tool in litigation in Brazil. It is rather common for lawyers to quote articles from renowned scholars, judges or reputable attorneys. These opinions, together with case law, usually serve as a strong persuasive argument.

As to the evidence a party may seek, the Code of Civil Procedure provides for three types of evidence: (i) documents, (ii) depositions and (iii) technical reports issued by court-appointed expert(s). All evidence must be presented by the parties to the judge and recorded in the dockets of the case. As opposed to the common law tradition, the judge, rather than the parties, is the one who actually inquiries the witnesses and experts. The oral evidence is taken during the trial and the counsels to the parties submit the questions to the judge, who, after scrutinizing the question, decides whether the witness will have to respond. Since the judge filters the questions before allowing the witnesses to give their answers, leading questions are commonly ineffective as they end up being rephrased by the judge. The parties have the right of cross-examining each other's witnesses but there is no rebuttal. Objections are theoretically feasible, but not very often used. In short, the judge controls the depositions.

The parties may present all kinds of documents; the general rule is that the complaint must bring all plaintiffs' documents and the defense all defendants' documents material to the dispute. After this initial phase the parties are precluded from bringing any document to the case unless it falls into the category of supervening events (whose evidence was not available at the time the brief was filed). Brazilian Procedural Law does not provide for the concept of an "expert witness." Facts whose full knowledge requires technical expertise are gathered through the use of a court-appointed expert. The use of one expert for each technical issue being raised in the case is permissible. The parties, however, refrain from requesting too many experts[33] to avoid the cost that entails.

The Code of Civil Procedure provides for some ancillary remedies[34] aimed at obtaining documents and things that are or should be in the other parties' possession (also applicable to third parties). The claimant must prove the existence of a legal or contractual relationship in connection with the party who is in possession of the document and shall also demonstrate that such document is material to the outcome of the dispute.

Fact-finding in Brazil is not nearly as intense as it may be in the pre-trial discovery available in common law jurisdictions. Brazilian Procedural Law provides for a system based on assumptions and distribution of the burdens of proof. Each party bears the burden of proving his/her own

[31] Contracts, family, consumer and torts law, corporate and securities laws, antitrust, federal taxes, administrative law, procedural law, insurance and reinsurance and so forth. A good side effect of having many bodies of law regulated by federal laws is that conflicts of law become a fairly simple subject.
[32] Introductory Law to the Civil Code lists (hierarchically) the sources of law: legislation, case law, general principles of law, analogy, custom and usage, equity and legal doctrine.
[33] Typically, there is only one expert.
[34] "Exhibition of Document" and "Search and Seizure." These proceedings are not used frequently.

allegations based on documents, witness or technical evidence. Undisputed facts (not challenged by the other party) are deemed established and the judge may decide based on such legal assumption.

Brazilian Law is no different from any other typical civil law of other countries when it comes to formalities. All communication from the court to the parties and between the parties is done through an official and formal channel. Communications are done either by a person representing the judiciary (a court official) or through the publication of the judge's decision on the official newspaper (official gazette). The requirement of resorting to public officers or media for communicating procedural acts is a major restriction to transnational litigation[35] and fact-findings in Brazil.

A major restriction to transnational litigation is the fact that Brazil is not a signatory to the Hague Convention on "Taking Evidence Abroad in Civil or Commercial Matters." As seen above, this convention is a material tool to secure evidence in foreign jurisdictions. In the absence of the Hague Convention, countries throughout the world ought to rely on Letters Rogatory[36] whenever alien courts wish to secure evidences in Brazil. This line of thought applies equally to service of process and taking of evidence.

As for the Americas, Brazil is a signatory[37] to the Inter-American Convention on 'Letters Rogatory'[38] and its "Additional protocol."[39] The advantage is that countries that are signatories to this convention are entitled to a direct and thus expedited communication with the applicable foreign court. Letters rogatory are usually transmitted via consular or diplomatic channels, which slow down the process as a whole. The direct communication provided for under the Inter-American Convention and its additional protocol tends to be considerably faster. It is worth noting that Brazil, although a signatory to the Inter-American Convention on "Taking of Evidence Abroad" has not ratified it to date, which makes its application moot in Brazil.

The main concern arising out of the issues mentioned above is the ultimate validity of the foreign judgment before Brazilian courts. After all, if the alien party or state seeking the service of process or the taking of evidence do not comply with the applicable Brazilian legislation, the chances of violating binding laws and public policy are considerable and the end result will probably be the failure to secure an exequatur from the court responsible[40] for ratifying the foreign judgment entered abroad. That is the main reason why it is always necessary to consider the perspective of both states involved.[41]

The 1988 Federal Constitution triggered a considerable debate among scholars over the courts reach on individual correspondence, data and telephone communications. The debate revolved over the issue of whether or not the secrecy of mail, telegraphic and data communications in general was absolute, that is, inviolable even for a court of law or similar body, as in the case of telephone communications. This understanding resulted from a literal interpretation of item XII of Article 5 of the 1988 Federal Constitution of Brazil, which says:

---

[35] Transnational litigation in this context means litigation commenced abroad involving Brazilian citizens as parties (or third parties) or, the opposite: litigation triggered in Brazil involving foreigners.

[36] Letters Rogatory (or letter of request) is a formal written request through which the courts of one country ask the courts of another country to utilize their procedure to assist the country making the request in the administration of justice within its borders. The most common remedies sought by Letters Rogatory are service of process and taking of evidence. *See* Black's Law Dictionary (letter of request).

[37] And most importantly, Brazil has ratified such convention.

[38] http://www.oas.org/main/main.asp?sLang=P&sLink=http://www.oas.org/legal/intro.htm.

[39] *ib. idem*.

[40] This task in Brazil has recently been transferred from the Federal Supreme Court (STF) to the Superior Court of Justice (STJ).

[41] Bermann, George A., Transnational Litigation, Thomson West, p. 262 (2003).

> the secrecy of mail and of telegraphic, data and telephonic communications is inviolable, except, in the last case, by court order, in the events and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts.

Because such provision contained "in the last case" referring specifically to telephone communications, some scholars construed that the other events were beyond the courts' reach. This understanding however did not prevail and the courts' general approach has been that the data secrecy is relative and thus it is inviolable unless a court order determines otherwise.

The party seeking to have access to evidence available in electronic format has to ask the court to secure the computer, hard-disk or the media where the evidence is stored.[42] The 1988 Federal Constitution[43] sets forth that the Public Administration has to manage government documentation and has to take necessary actions to facilitate the consultation for those who may need them. Law 8.159/91, enacted three years later, regulated the constitutional provision mentioned above and determined the guidelines of a broad public policy on public and private archives.

Apart from those regulations, which are aimed at the preservation of public files, Brazilian law does not have a specific provision towards the retention of private documentation. Rather, retention of documents in Brazil is usually perceived as a self-defense maneuver against future disputes. For this reason private firms and people in general bear in mind the relevant statute of limitation to assess the amount of time they should retain their documents.

For example, tax laws provide for a generic 5-year term statute of limitations. This is a term commonly observed by companies in Brazil. Certain organs have prepared the so-called "Retention Tables" in an effort to provide some guidance to companies. However, these tables derive from mere interpretation of possible statutes of limitation that may apply to each document.

The Brazilian Federal Constitution sets forth that "the privacy, private life, honor and image of persons are inviolable, and the right to compensation for pecuniary damages and pain and suffering resulting from their violation is ensured."[44]

The home is rendered "inviolable" by the Constitution which sets forth that "no one may enter therein without the resident's consent, except in the event of *flagrante delicto* or disaster, or to give help, or, during the day, by court order."[45]

As seen above, the Federal Constitution also protects the confidentiality of mail and electronic communication, except by court order "for purposes of criminal investigation or criminal procedural fact-finding procedures."[46] Although the Constitution mentions criminal judges only, "court order" should be understood broadly since all judges (civil/commercial, tax, labor and so forth) are empowered to rely on this provision.

Another aspect covered by the Federal Constitution is the protection of sources: "access to information is ensured to everyone and the confidentiality of the source[47] shall be safeguarded, whenever necessary for the professional activity."

---

[42] The Code of Civil is quite liberal on admissible evidence. The governing provision is Article 332: "All legal means, as well as those morally acceptable, even if not particularly specified in this Code are admitted as evidence to show the veracity of the facts on which the complaint or the answer are based upon."

[43] Federal Constitution, paragraph two of Article 216.

[44] Item X of Article 5 of the 1988 Federal Constitution of Brazil: X.

[45] Item XI of Article 5 of the 1988 Federal Constitution of Brazil: XI.

[46] Item XII of Article 5 of the 1988 Federal Constitution of Brazil: XII - The secrecy of mail and of telegraphic data and telephone communications is inviolable, except, in the last case, by court order, in the events and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts.

One may infer from these provisions that the individual privacy has a Constitutional status. The general rule is that privacy is safeguarded unless a court order determines otherwise. Wiretapping is a good example of the courts' reach on privacy issues. Law 9.296/96 allows wiretapping for a period of 15 days, renewable for another 15 days upon a judge's order. Wiretapping is allowed only in cases where the police force suspects serious crimes punishable by imprisonment, such as murder, kidnapping, drug and contraband smuggling and corruption.

Many statutes have been enacted to increase and further regulate the aforementioned constitutional provisions. Consumer Protection Code,[48] for instance, sets out a number of rules concerning consumer-related data. Financial information has been extensively regulated in view of competing values: consumer's privacy and information on credit worthiness.[49] The Consumer Protection Code also sets forth that once the consumer has settled his/her debts, Credit Protection Services shall not provide any information that may prevent or hinder further access to credit for that consumer.[50]

Brazilian Courts tend to deem unlawful a recorded conversation if one of the parties was unaware of the recording. However, if a given fact would be considerably difficult of being evidenced (such as family cases, pre-contractual arrangements or oral agreements), courts are increasingly (and quite exceptionally) admitting such kind of evidence to be used.

Precedents on privacy concerning e-data:

Brazilian Labor Law has so far addressed the protection of privacy and personal information in the workplace in a very limited way.[51] As the protection of privacy and personal information has become a great concern in the workplace, the volume of case law addressing this issue has substantially increased.

A good example is case law addressing the employer's right to monitor employee's email communication over the company email system. In *Elieson Nascimento v. HSBC Seguros Ltd.* (the only case that has been taken to the Superior Labor Court so far), defendant (HSBC) found out through monitoring that an employee was sending pornographic pictures over the company's email system. As a result, the employee, Elieson Nascimento, was dismissed for cause.[52] He filed a lawsuit (labor claim) alleging that his termination for cause should be deemed void on the grounds that the employers violated his privacy by monitoring his emails.

According to the Superior Labor Court: (i) the computer, the access to the internet and to the company e-mail system were only provided to the employee in order to allow him to perform his duties; (ii) the employer has the right to monitor its own email system in order to avoid any damages that might come from the inappropriate use of the company email by the employee. Therefore, Superior Labor Court held that there is no reasonable expectation of privacy in the emails

[47] Protection of sources is an issue that has received more attention after William Mark Felt revealed his identity ("Deep Throat") and the incident involving Valerie Plame, and journalists Judith Miller and Matt Cooper became public.

[48] The Consumer Protection Code provides that consumers shall have access to personal data, consumer files and other information stored in files, and databases about themselves, as well as about the sources of these data. Also, consumer files and data shall be objective, clear, true, easily comprehensible, and shall not contain deprecating information regarding periods prior to five years. In addition, the opening of a consumer file, archive, registry, or database should be communicated in writing to the consumer, if not opened at the consumer's behest. Also, whenever consumers find that data and files about them are incorrect, they may demand immediate correction, and whoever in charge of the file shall communicate the due corrections within five days.

[49] Complementary Law No. 105, January 10, 2001.

[50] Paragraph 5 of Article 43.

[51] Federal Law no. 9.029/95 limits the medical exams that may be required to job applicants. For instance, pregnant tests or HIV tests are not allowed.

[52] Meaning that he was prevented from receiving some social rights (termination package) that he would be entitled to had his labor agreement been terminated *without* cause.

communications over the company email system.[53] Labor law scholars suggest employers to notify their employees in writing of their intent to monitor the e-mails as well as to instruct employees of the company's rules on the use of internet/email.

Mutual Legal Assistance Treaties for investigation are also an important source for cross-border discovery. When it comes to the execution of rogatory letters, the provisions of Article 105, I, "i" of the Federal Constitution sets forth the competence of the Brazilian Federal Supreme Court to process and judge the homologation of foreign decisions. The Federal Police also may fill foreign orders and cooperate with international organisms.

[53] This decision mentioned three United States precedents: *O'Connor v. Ortega 480 U.S. 709; Bourke v. Nissan Motor Corp. No.B068705 (Cal. Ct. App., July 26,1993)* and *Smyth v. Pillsbury Co.914 F. Supp. 97, 101 (E.D. Pa. 1996)*

Canada

Kelly Friedman - ***Lead Editor***
Dominic Jaar, Susan Wortzman, Robert Deane, Azim Hussein, Paul Robertson - ***Contributing Editors***
Dan Michaluk, Bushra Rehman- ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Canada has a federal system of government; that is, the authority to make laws is divided between the government of Canada and the provincial/territorial governments. The legal division of powers is found in the Constitution Act, 1867. The powers of the provinces/territories are specifically listed in section 92 of the Constitution Act, 1867. The federal government exercises most remaining constitutional powers under its residual power to ensure "Peace, Order and Good Government." While there are some areas of shared jurisdiction, in general, the federal government legislates with regard to matters that affect all of Canada, such as the criminal law, inter-provincial trade, telecommunications, immigration and fisheries. The provinces and territories make laws in areas such as education, property, civil rights and the administration of justice within their borders.

   With respect to matters within provincial jurisdiction, Canada's legal system is "bijural": all provinces and territories are governed by the common law, with the exception of the province of Québec, which is a civil law jurisdiction. Québec's private law is principally governed by the Civil Code of Québec, which has its roots in the French Napoleonic Code and French civil law more generally.

   There is a Federal Court in Canada which is a national trial and appellate court which hears and decides certain legal disputes arising in the federal domain, including claims against the government of Canada, civil suits in federally-regulated areas and challenges to the decisions of federal tribunals. Its authority derives primarily from the Federal Courts Act. It was created in 1971 under the authority of s. 101 of the Constitution Act, 1867 for the "better administration of the laws of Canada" and is the heir of the former Exchequer Court created in 1875. With respect to disputes resolved in the Federal Court, the law relating to document disclosure is regulated by the Federal Courts Rules, and it is developed by decisions of the Federal Court and Federal Court of Appeal.

   With respect to matters in the jurisdiction of the provincial/territorial courts, in the common law provinces, the law relating to document discovery is regulated by the various provincial/territorial rules of court. Courts are frequently asked to interpret these various rules in pre-trial rulings. This has resulted in a well-developed body of case law.

   The rules of many of the provinces are substantially similar, and two territories have adopted the rules of other provinces. In virtually every Canadian jurisdiction, the definition of "document" in the applicable court rules is defined to include, or at least contemplate, electronically stored information.

   In the province of Québec, the law relating to the disclosure of documents to other parties and the production of exhibits in the court record is regulated by the Code of Civil Procedure. As in the other provinces and

territories, Québec courts are frequently asked to interpret these various rules in pre-trial rulings. Further, in An Act to establish a legal framework for information technology , a "document" is any information inscribed on a medium including information on a technology-based medium.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

Common Law Jurisdictions:

Generally, Canadian common law jurisdictions impose broad discovery obligations. In general, disclosure must be made of every document relating to any matter in issue in the action that is or has been in the possession, control or power of a party. This applies even if privilege is claimed in respect of the document, in which case disclosure must be made of the document's existence but not its contents. In all jurisdictions, "document" is broadly defined to include electronically stored information.

In each jurisdiction, "relevance" is a prerequisite for the production obligation to arise. For example, the British Columbia Supreme Court Rules provide that every document relating to any matter in question in the action shall be disclosed. Rule 186.1 of the Alberta Rules of Court requires that disclosed records be both relevant and material. Under Ontario Rule 30.03(1), every party is required to serve an Affidavit of Documents disclosing, to the full extent of the party's knowledge, information and belief, all documents relating to any matter in issue in the action that are or have been in the party's possession, control or power. The Affidavit of Documents lists and describes, in various schedules, relevant documents which will be produced in the litigation, documents no longer in the party's possession and documents over which privilege is claimed. Where privilege is claimed, the grounds for the claim of privilege are to be stated, along with the nature of the document, its date, and other details sufficient to identify the document.

The disclosure obligations are ongoing and continuous. Omissions to the Affidavit of Documents must be corrected when discovered, and additional documents discovered after the original Affidavit was sworn must be listed in a supplementary Affidavit of Documents.

Québec:

The discovery rules in Québec are more similar to discovery rules in the United States than to those in the rest of Canada. The Code of Civil Procedure requires litigants to make specific requests for production. There is no proactive obligation on a party to disclose documents, except for those exhibits in the party's possession that it relies on in support of its action or defence, and/or intends to refer to at the hearing.

The "discovery" phase of a Québec court case is referred to as "special proceedings relating to production of evidence" in the Code of Civil Procedure. It runs from the moment the introductory motion is filed in the court docket and served on the other parties until the end of the hearing. However, all documents which a plaintiff intends to refer to at the hearing must be disclosed to all other parties when the case is inscribed for proof and hearing. The other parties must do likewise within 30 days after the inscription, failing which any exhibit to which they may wish to refer may be filed only with the permission of the court.

A defendant may, before filing a defence, summon the plaintiff or a representative of the plaintiff, or with the permission of the court, any third party, to be examined upon all facts relating to the issues raised by the introductory motion or to provide document disclosure and allow a copy to be made of any document relating to the issues.

After a defence is filed, any party may summon any other party or a representative of the party, or with the permission of the court, any third party, to be examined upon all facts relating to the issues between the parties or to give disclosure and allow copy to be made of any document relating to these issues. The court may also, at any time after a defence is filed, order a party or a third person having in their possession any real evidence relating to the issues between the parties to exhibit it, preserve it or submit it to an expert's appraisal.

Further, anyone who, expecting to be a party to a legal proceeding, has reason to fear that evidence may be lost or become more difficult to obtain may, by motion, request that the evidence be examined by a person of their choice.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Common Law Jurisdictions:

There is no right to obtain pre-action disclosure or disclosure from non-parties in the Canadian common law jurisdictions. However, the court may grant leave to obtain pre-action or non-party disclosure under specific circumstances. If such an order is granted, the subject of the order must comply with the order, as with any other court order, failing which contempt proceedings can be brought.

With respect to pre-action disclosure, an "equitable bill of discovery" may be granted by a court to permit a plaintiff to obtain a defendant's identity prior to the commencement of a law suit if the applicant can establish: a prima facie case against the unknown alleged wrongdoer; the person from whom the disclosure is sought is more than an innocent bystander; that person is the only practical source of the information sought; that person will be reasonably compensated for expenses arising out of compliance with the discovery order; and the public interest in favour of disclosure outweighs legitimate privacy concerns.

With respect to discovery of non-parties, the common law provinces permit a party to seek, on motion to the court, an order requiring third parties to produce documents in their possession, control or power (over which privilege is not claimed) for inspection or to submit to an examination under oath. The test to obtain such an order is quite stringent. For example, Rule 31.10 of the Ontario Rules of Procedure provides that a court shall not grant leave to examine a non-party unless the court is satisfied that the party has been unable to obtain the information from persons they were otherwise entitled to examine; it would be unfair to require the moving party to proceed to trial without the information sought; and the examination will not unduly delay the commencement of trial, entail unreasonable expense for other parties or result in unfairness to the non-party. Any such order granted will usually be specific as to the information which must be provided so as to prevent unfairness to the non-party.

With respect to both pre-action disclosure and disclosure from non-parties, in certain circumstances, Canadian privacy legislation can be used to obtain disclosure. In particular, a party has a right to have access to its personal information in the possession or control of an entity unless a specific exception to access is found in the relevant privacy legislation. It is also possible to use access to information laws to obtain records from public bodies.

Québec:

After a defence is filed, any party may, with the permission of the court, summon a non-party or a representative of the non-party, to be examined upon all facts relating to the issues between the parties or to provide disclosure and allow a copy to be made of any document relating to the issues. If, after a defence is filed, a document relating to the issues between the parties is determined to be in the possession of a third

party, they may, upon summons authorized by the court, be ordered to give disclosure of it to the parties. Further, the court may also, at any time after a defence is filed, order a party or a third person having in their possession any real evidence relating to the issues between the parties to disclose or preserve it.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

Common Law Jurisdictions:

The rules of procedure applicable in the common law jurisdictions do not expressly impose preservation obligations on potential parties to litigation in respect of relevant documents. If litigation is not anticipated, individuals/corporations may destroy documents in the normal course of business, subject to any obligations to retain documents for regulatory or statutory purposes. However, a party may face claims of spoliation (intentional destruction of information relevant to issues in the litigation) if it is discovered that relevant information was destroyed when litigation ought to have been reasonably anticipated.

Québec:

At the present time, it is not clear whether any specific obligation to preserve evidence exists beyond the general obligation of parties, as prescribed by the Civil Code of Québec, to refrain from acting in a way that causes prejudice to another person or behaving in an excessive or unreasonable manner, contrary to the requirements of good faith. Beyond this basic obligation, there are two opposite theories:

1) *No obligation to preserve*

   According to the Civil Code of Québec, ownership is the right to use, enjoy and dispose of property fully and freely, subject to the limits and conditions for doing so as determined by law, for example, fiscal and privacy laws. This would mean anyone can destroy any document which is its property so long as there is no specific legislative requirement to retain it, except if the destruction occurs with the intent of causing prejudice to another person.

2) *Obligation to preserve*

   An obligation to preserve is premised on the duty of every person to abide by the rules of conduct so as not to cause injury to another. On this theory, destruction of a potentially relevant document should be a delict, or tort in common law parlance, if it causes damage to another person, regardless of the good or bad faith of the person destroying the document.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

Common Law Jurisdictions:

If a litigant is found to have spoliated evidence (by withholding, hiding, or destroying evidence relevant to litigation), the court may draw an adverse inference such that the court may infer that the documents which have not been preserved would have assisted the opposite party to the litigation. Other potential sanctions include cost awards or the court's ability to strike a part or the entirety of the offending party's pleadings or an outright dismissal of a party's claim. If the misconduct is characterized by the court as an independent tort, as opposed to a failure to abide by the Rules of Court, other remedies, such as an award of damages, may follow.

Principle 11 of the Sedona Canada Principles provides that sanctions should be considered by the court where a party will be materially prejudiced by another party's failure to meet any obligation to preserve, collect, review or produce electronically stored information. The party in default may avoid sanctions if it demonstrates the failure was not intentional or reckless.

Québec:

In Québec, a pending case is likely to address the issue of whether there is a rebuttable presumption that the evidence destroyed by a party would have been adverse to that party's interest. There is also the possibility that the court will treat spoliation as an independent delict and award damages. As with any delict in Québec, damages compensate for losses sustained and profits deprived.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

Common Law Jurisdictions:

In Canada, the producing party generally bears its own costs of preserving, collecting, reviewing and producing relevant documents and evidence. The receiving party is generally responsible for the immediate costs of copying, binding and delivery of the documents to it.

Any cost-shifting generally occurs at the end of the litigation, at which time the unsuccessful litigant may be required to contribute, in whole or in part, towards the fees and disbursements of the successful party. This is often referred to as a "loser pays" system. While cost-shifting in cases involving electronically stored information has been proposed, to date, Canadian courts have not deviated significantly from the traditional regime.

Québec:

Costs of discovery/disclosure in the province of Québec are treated similarly as in the rest of Canada, however, the costs of discovery in Québec are generally not as significant as in the common law provinces as discovery tends to be more limited. As with the common law jurisdictions, the producing party generally bears its own costs of preserving, collecting, reviewing and producing relevant documents and evidence. The receiving party is generally responsible for the immediate costs of copying, binding and delivery of the documents to it, however, the producing party generally assumes these costs on an interim basis. After the final judgment, the losing party has to contribute towards the fees and disbursements of the successful party based on a prescribed tariff that does not reflect the actual costs of litigation.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

The provincial/territorial/federal rules of court and in Québec, *An Act to establish a legal framework for information technology*, define "document" to include, or at least contemplate, electronically stored information.

The body of case law relating to e-discovery is growing in Canada. Summaries of e-discovery cases are located on the Ontario Bar Association website as follows:

Common Law: http://www.oba.org/en/main/ediscovery_en/digest.aspx

Québec Civil Law: http://www.oba.org/en/main/ediscovery_en/quebec.aspx

Additionally, there are Practice Directions in the provinces of British Columbia and Alberta regarding the production of electronic evidence, and there are Guidelines regarding the production of electronically stored information in Ontario. It is expected that some of the common law jurisdictions will endorse or adopt the *Sedona Canada Principles* through Practice Directions or Rule amendments.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

Common Law Jurisdictions:

The rules of court in the common law jurisdictions contemplate the disclosure of electronic documents. For instance, Rule 30.01(1)(a) of the Ontario *Rules of Civil Procedure* defines "document" to include: "a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account, and data and information in electronic form." This interpretation builds on the definitions in Rule 1.03(1) which defines "document" to include "data and information in electronic form" and "electronic" to include "created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means, and 'electronically' has a corresponding meaning." The Guidelines for the Discovery of Electronic Documents in Ontario (the "Ontario Guidelines")[54] provides that "Generally speaking, documents are referred to as 'electronic' if they exist in a medium that can only be read through the use of computers, as distinct from documents that can be read without the aid of such devices." The British Columbia rules define "document" as follows: "'document' g of sound, any record of a permanent or semi-permanent character and any information recorded or stored by means of any device."[55] A Practice Direction applicable to civil actions in the Supreme Court British Columbia[56] defines "electronic material" as follows:

> Any material including but not limited to e-mails, computer generated files including any disk, tape, sound track or other device in which sounds or other *Data* [defined term] are recorded and any film (including microfilm), negative, tape or other device in which one or more visual images are embodied which is identified in its *Native Format* [defined term]. An example is a computer file for a Microsoft Word document rather than the printed version of the document or the *Data* captured when a digital camera takes a picture rather than the printed version of the picture or the computer file created when a digital dictation machine records a voice.

The *Canada Evidence Act* provides that any party who wants to tender an electronic document in a criminal proceeding, any civil proceeding or other matter over which the Federal Government has jurisdiction, must authenticate the document. It defines "electronic document" to include "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."[57] Provincial Evidence Acts contain similar definitions. For instance, the Ontario *Evidence Act* defines "electronic record" to be "data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that data, other than a printout referred to in subsection (6)."[58]

[54] Available online at http://www.oba.org/en/main/ediscovery_en/default.aspx.
[55] B.C. Reg. 221/90, R.1(8).
[56] Practice Direction Re: Electronic Evidence, available online at http://www.courts.gov.bc.ca.
[57] *Canada Evidence Act*, R.S., 1985, c. C-5, s. 31.8.
[58] *Evidence Act* (Ontario), R.S.O. 1990, Chapter E.23.

The *Sedona Canada Principles* provide that electronically stored information is "electronic" if it exists in a medium that can be read through the use of computers or other digital devices.

Québec:

Article 3 of *An Act to establish a legal framework for information technology* states the following:

> Document: Information inscribed on a medium constitutes a document. The information is delimited and structured, according to the medium used, by tangible or logical features and is intelligible in the form of words, sounds or images. The information may be rendered using any type of writing, including a system of symbols that may be transcribed into words, sounds or images or another system of symbols.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

Common Law Jurisdictions:

The Rules of Court applicable in the common law jurisdictions generally do not require the parties to meet and confer, although the Practice Directions of British Columbia and Alberta and the Ontario Guidelines encourage it.

Principle 3 of the *Sedona Canada Principles* expressly endorses the concept of "meet and confer":

> Counsel and parties should meet and confer as soon as practicable and on an ongoing basis, regarding the identification, preservation, collection, review and production of electronically stored information.

Principle 8 of the Ontario Guidelines is very similar, and provides as follows:

> Counsel should meet and confer, as soon as practicable and on an ongoing basis, regarding the location, preservation, review and production of electronic documents, and should seek to agree on the scope of each party's rights and obligations with respect to e-discovery, and a process for dealing with them.

Ontario courts have endorsed this approach.[59] The Federal Court has also encouraged the parties to meet and confer.[60]

Québec:

In Québec, modifications to the *Code of Civil Procedure* have introduced the notion of "meet and confer" by requiring the parties to agree on the conduct of the proceeding after the filing of the introductory motion. The agreement must cover, among other things, the procedure and time limit for the disclosure of exhibits.[61]

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

Common Law Jurisdictions:

The comments with respect to the preservation of documents set out in response to question 4 are applicable in the electronic discovery context. In addition, principles and guidelines developed to give parties practical guidance for e-discovery purposes and utilized by Canadian courts are all consistent in that they require potential litigants to preserve relevant electronically stored information. However, the general obligation to

[59] *See*, *e.g., JDS Uniphase Inc. v. Metconnex Canada Inc.*, 2006 CanLII 34432 (ON S.C.).
[60] *See*, *Canada (Commissioner of Competition) v. Air Canada* (T.D.), [2001] 1 F.C. 219, 2000 CanLII 17157 (F.C.).
[61] *Code of Civil Procedure*, R.S.Q. c. C-25, ss. 151.1 - 151.23.

preserve electronically stored information is balanced against the party's right to manage its electronically stored information in an efficient manner. The threshold does not require litigants to take "every conceivable step" to preserve potentially relevant electronically stored information. It is generally sufficient that parties make reasonable inquiries based on a reasonable and good faith attempt to identify and preserve electronically stored information.

The debate with respect to whether there is an obligation to preserve documents set out in response to question 4 is equally applicable in the electronic discovery context.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

Common Law Jurisdictions:

The comments with respect to the obligation to disclose relevant documents set out in response to question 2 are applicable in the electronic discovery context.

The *Sedona Canada Principles* give further guidance to the parties in respect of electronically stored information. Principle 4 provides that "as soon as litigation is reasonably anticipated, parties must consider their obligation to take reasonable and good faith steps to preserve potentially relevant electronically stored information," and Principle 5 provides that "the parties should be prepared to disclose all relevant electronically stored information that is reasonably accessible in terms of cost and burden."

Québec:

A party has no obligation to search for any type of document, unless the request is for a relevant document, or the party is ordered to do so by the court or by subpoena or when, in the course of an examination on discovery, the party undertakes to search for particular documents.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

Common Law Jurisdictions:

The common law jurisdictions in Canada require the production of an Affidavit of Documents or an unsworn List of Documents with accompanying schedules or lists of documents, described in response to question 2. The Affidavit or List of Documents function as formal confirmation by a party that it has searched for all relevant documents, including electronic documents, in respect of the litigation.

Québec:

No such rule exists.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

While there is no legal provision or rule in this regard, there is some guidance given to parties to Canadian litigation. Principle 11 of the Ontario Guidelines provides that a party must produce a document in electronic form if, for the purposes of the litigation, it is not sufficient to produce the traditional paper version of the document. The Practice Direction applicable to civil actions in the Supreme Court of British Columbia refers

parties to the Ontario Guidelines when considering a protocol regarding the collection and discovery of electronic material and prescribes a default protocol governing the form of production.[62]

Further, Principle 8 of the *Sedona Canada Principles* provides as follows:

> Parties should agree as early as possible in the litigation process on the format in which electronically stored information will be produced. Parties should also agree on the format, content and organization of information to be exchanged in any required list of documents as part of the discovery process.

Canadian courts have confirmed that information printed as a hard copy may be insufficient and endorse production of information in electronic format when it is available.[63]

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

Common law – duty to collect, filter and produce

In collecting, filtering and producing electronic information, litigants in Canadian common law jurisdictions are subject to a diligence standard. This duty is derived from the requirement to swear an affidavit of documents in a specific form, which in most jurisdictions includes a statement by which an affiant affirms that he or she has conducted a "diligent search."[64] Breach of the duty to conduct a diligent search will not necessarily lead a court to order a party to conduct a further and better search or make other remedial or punitive orders. Such orders are discretionary and are made based on a broad range of factors, including whether a further and better search is proportional and whether a party has been prejudiced by non-disclosure.

Common law – duty to preserve

Though most would agree that Canadian litigants must take reasonable steps to preserve producible records, given the roots of the spoliation doctrine in Canada the exact standard of conduct for preserving documents is not yet clear.

St. Louis v. Canada is the foundation for the doctrine of spoliation in the Canadian common law jurisdictions.[65] In *St. Louis*, the Supreme Court of Canada held that the spoliation presumption – "all things are presumed against a wrongdoer" – is an evidentiary doctrine that may justify a presumption of fact.[66] This means a spoliation-based adverse inference can be rebutted by other evidence. It also means the strength of the presumption will vary based on the circumstances in which evidence has been destroyed. On this traditional view, a litigant's duty is to refrain from intentionally destroying relevant evidence.

Canadian courts may also address spoliation issues on bases other than evidentiary. Namely, courts may address spoliation as part of their power to supervise the discovery process or as an independent actionable wrong. These bases for addressing spoliation justify a positive duty to preserve evidence subject to a reasonableness or due diligence standard of conduct. An express positive duty to "take measures to preserve" electronic evidence is now featured in the Nova Scotia Supreme Court rules, the first court rules in Canada to specifically address e-discovery.[67] And though the spoliation doctrine still requires significant development and clarification, Canadian

[62] Practice Direction Re: Electronic Evidence, s.4.3.1, available online at http://www.courts.gov.bc.ca.

[63] *See*, *e.g., Cholakis v. Cholakis* (2000), 44 C.P.C. (4th) 162 (Man. Q.B.): "The plaintiff has satisfied me that the electronic information requested falls within the definition of a document under the Rules and contains relevant information that should be produced. If the defendants Leo Cholakis, Fairmont Real Estate Limited and Kensington Building Limited wish to provide the information in a format that does not reveal irrelevant information, then it is incumbent upon them to develop a mechanism by which that can be done. The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

[64] *See*, *Air Canada v. Westjet* (2006), 81 O.R. (3d) 48 (S.C.J.) and *Eli Lily Canada Inc. v. Nopvopharm Ltd*. (2007), 63 C.P.R. (4th) 1 (F.C.) as to the nature and scope of this duty.

[65] *St. Louis v. Canada* [1896], 25 S.C.R. 649.

[66] *Ibid.*

[67] Nova Scotia Supreme Court Rule 16.03.

courts in common law jurisdictions have held that litigants have a positive duty to take reasonable steps in preserving electronic records.[68]

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

Solicitor-client privilege is accorded the utmost respect by Canadian courts. In 2006, the Supreme Court of Canada stated as follows with regard to its importance:

> Much has been said in these cases, and others, regarding the origin and rationale of the solicitor-client privilege. The solicitor-client privilege has been firmly entrenched for centuries. It recognizes that the justice system depends for its vitality on full, free and frank communication between those who need legal advice and those who are best able to provide it. Society has entrusted to lawyers the task of advancing their clients' cases with the skill and expertise available only to those who are trained in the law. They alone can discharge these duties effectively, but only if those who depend on them for counsel may consult with them in confidence. The resulting confidential relationship between solicitor and client is a necessary and essential condition of the effective administration of justice.[69]

Canadian courts have generally accepted that solicitor-client privilege is not waived through inadvertent disclosure.[70] Canadian courts expect counsel and their clients to carefully guard the privilege, however, and have ruled that parties must employ reasonable good faith efforts to detect and prevent the production of potentially privileged information.[71]

Principle 9 of the *Sedona Canada Principles* provides that:

> During the discovery process parties should agree to, or if necessary, seek judicial direction on, measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronic documents and data.

Where counsel has obtained privileged disclosures from an opposing party and has failed to return them even though it is apparent that the disclosure was inadvertent, ethical issues arise and sanctions may be imposed on the receiving counsel. These sanctions can include striking pleadings, the removal of counsel from the file and costs. The removal of counsel has been ordered where the evidence demonstrated that counsel knew or should have known that it had inadvertently been provided with the opposing party's solicitor-client communications but took no steps to seek directions from the court or to stop the review and notify the privilege holders.[72]

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

Cost-shifting in cases involving electronically stored information has been proposed, to date, Canadian courts have not deviated significantly from the traditional regime which is discussed in question 6.

---

[68] *See, e.g., Dickson v. Broan NuTone Canada Inc*., [2007] O.J. No. 5114 (S.C.J.) (QL) (where the court reviewed the conflicting duty on the standard of conduct).
[69] *Blank v. Canada (Minister of Justice)*, [2006] 2 S.C.R. 319, 2006 SCC 39 (CanLII) at para. 26.
[70] *See Elliot v. Toronto (City)* (2001), 54 O.R. (3d) 472 (Sup. Ct.) at para. 10; John Sopinka, Sidney N. Lederman & Alan W. Bryant, *The Law of Evidence in Canada*, 2nd ed. (Toronto: Butterworths, 1999) at 766-7; *Dublin v. Montessori Jewish Day School of Toronto*, 2006 CanLII 7510 (Ont. Sup. Ct.); *Sommerville Belkin Industries Ltd. v. Brocklesh Transport and Others* (1985), 65 B.C.L.R. 260 (S.C.); *National Bank Financial Ltd. v. Daniel Potter et al.* (2005), 233 N.S.R. (2d) 123 (S.C.), 2005 NSSC 113 (CanLII); *National Bank Financial Ltd. v. Daniel Potter* (2004), 224 N.S.R. (2d) 231 (S.C.), 2004 NSSC 100 (CanLII); *Autosurvey Inc. v. Prevost*, 2005 CanLII 36255 (Ont. Sup. Ct.).
[71] *See Air Canada v. Westjet Airlines Ltd*. (2006), 267 D.L.R. (4th) 483 (Ont. Sup. Ct.) wherein the court rejected the request for an order protecting against the waiver of privilege where a "quick peek" type of production was being proposed.
[72] *See National Bank Financial Ltd. v. Daniel Potter* (2005), 233 N.S.R. (2d) 123 (S.C.), 2005 NSSC 113 (CanLII); *Auto Survey Inc. v. Prevost,* 2005 CanLII 36255 (Ont. Sup. Ct.); *Celanese Canada Inc. v. Murray Demolition Corp.* (2006), 269 D.L.R. (4th) 193 (S.C.C.), 2006 SCC 36 (LexUM).

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

All of the above-mentioned tools are becoming increasingly common in Canada to ensure preservation of electronic information. The Sedona Canada Principles,[73] released in January 2008, clearly recommends each of these tools as best practices. Further, Canadian courts increasingly note that properly run business must have such policies and tools in place to defend against allegations of spoliation of evidence. For instance, in *Moezzam Saeed Alvi v. YM Inc. (sales)*, 2003 CanLII 15159 (ON S.C.) the court recognized the importance of records retention policies, as follows:

> . . . a properly run company should have a documents retention policy requiring retention of files for a reasonable period extending beyond the limitation period for civil cause of action in contract or tort and the limitation period for a reassessment under the Income Tax Act. A failure to do so risks a court making an adverse inference on the absence of evidence (para 48).

In *Jay v. DHL*, 2008 PEISCTD 13 (CanLII), the importance of the litigation hold was underscored. The court dismissed the defendant's statement of defence and recommended that the plaintiff move for default judgment because the defendant had not suspended its policy of destroying waybills after 9 months even though the plaintiff had specifically requested waybills.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The use of technology to assist in the e-discovery process is growing as described in the answer to question 17. Organizations are looking to records management and archiving to proactively manage retention and expiry of information. Reactively search and analytics technologies are being used to respond to discovery or search requirements.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

The privacy of parties and non-parties who may be affected by discovery-related obligations is protected in Canada by the "implied undertaking" – a rule by which all civil litigants undertake not to use information obtained through the discovery process for a collateral purpose without consent or leave. There are two purposes for the rule: (1) to provide for a reasonable degree of personal privacy in a civil justice system that compels disclosure of private information and (2) to further the administration of justice by encouraging complete and candid discovery.[74]

Though the implied undertaking rule is based in the common law, it has now been codified with particularity in some jurisdictions' court rules.[75] The Ontario *Rules of Civil Procedure*, for example, specify that the undertaking applies to evidence obtained in discovery and "information obtained from evidence [obtained in discovery]."[76] The Ontario Rules also make clear (1) that the undertaking ceases to apply once evidence is filed in court and (2) that the undertaking does not prevent the use of evidence to impeach a witness in a subsequent proceeding.[77]

---

[73] The Sedona Canada Principles Addressing Electronic Discovery, The Sedona Conference® Working Group 7, January 2008.
[74] *Juman v. Doucette*, 2008 SCC 8 at paras. 23 – 28 [*Juman*].
[75] *See*, *Queen's Bench Rules*, M.R. 553/88, r. 30.1, *Rules of Civil Procedure*, R.R.O., Reg 200, r. 30.1 [Ontario Rules] and *Rules of Civil Procedure*, r. 30.1 (Prince Edward Island).
[76] Ontario Rules, *ibid.*, r. 30.1.01(1)(b).
[77] *Ibid.*, r. 30.1.01(4).

In Ontario and elsewhere, a supervising court has the power to relieve against the undertaking where the interest of justice outweighs the prejudice that would result to a party who disclosed the evidence.[78]

Though it is still debatable whether the defendants to regulatory and criminal charges are subject to the same implied undertaking as civil litigants,[79] it is clear that they must follow a mandatory common law screening process before producing materials from the Crown in a criminal or regulatory prosecution to an opponent in litigation. The leading case is *D.P. v. Wagg*, where the Ontario Divisional Court established the following screening process:

- The party in possession or control of the Crown brief must disclose its existence in the party's Affidavit of Documents and describe in general terms the nature of its contents.
- The party should object to produce the documents in the Crown brief until the appropriate state authorities have been notified, namely the Attorney General and the relevant police service, and either those agencies and the parties have consented to production, or on notice to the Attorney General and the police service and the parties, the Superior Court of Justice has determined whether any or all of the contents should be produced.
- The judge hearing the motion for production will consider whether some of the documents are subject to privilege or public interest immunity and generally whether "there is a prevailing social value and public interest in non-disclosure in the particular case that overrides the public interest in promoting the administration of justice through full access of litigants to relevant information."[80]

Though the "Wagg process" is a common law process, there is some discussion about codifying it in court rules.[81]

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

Canada has a number of federal and provincial data protection statutes with plenary data protection codes that regulate the collection, use, disclosure, storage, retention and disposal of personal information. The coverage of Canadian data processing activity is fairly broad but not complete, and given the number of Canadian data protection statutes, threshold questions about statutory application are common in managing Canadian data protection issues.

There are four types of Canadian data protection regulation: commercial sector regulation, public sector regulation, employment regulation and health sector regulation.

Commercial sector data protection regulation

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[82] regulates the collection, use and disclosure of personal information in the course of commercial activity in all provinces except for British Columbia, Alberta and Quebec. These three provinces have passed their own

[78] *Juman*, *supra* note 74, at para. 34.
[79] *P. (D.) v. Wagg* (2004), 239 D.L.R. (4th) 501 at 520 (Ont. C.A.).
[80] *P. (D.) v. Wagg* (2002), 22 D.L.R. (4th) 97 (Ont. Div. Ct.), allowed in part (2004), 239 D.L.R. (4th) 501 (Ont. C.A.) (screening process is as articulated by the Court of Appeal).
[81] *See* D. Dwyer, *Report on the Working Group on The Collateral Use of Crown Brief Disclosure* (Charlottetown: Uniform Law Conference of Canada Joint Civil and Criminal Sections, 2007).
[82] S.C. 2000, c. 5 [PIPEDA].

commercial sector data protection statutes which have been declared "substantially similar" to PIPEDA[83] and therefore replace PIPEDA for their full scope of application.

Public sector data protection regulation

Canadian federal, provincial and municipal governments are subject to data protection codes imposed by legislation. Most of the federal government's data processing activity, for example, must be conducted in accordance with the federal *Privacy Act*.[84] Each province has passed similar legislation that applies to provincial and municipal governments and most of their boards and agencies.

Employment data protection regulation

The application of employee privacy regulation depends partly on whether employment is in the public or private sector. Most Canadian public sector employees are protected by public sector data protection legislation.[85] Private sector employees in British Columbia, Alberta, Quebec and employees of federally-regulated employers (banks, telecommunications and inter-provincial transport companies, for example) are protected by the commercial sector data protection legislation in each jurisdiction. Private sector employees in other Canadian provinces who are not employed by federally-regulated employers (the vast majority of employers in Canada) have no such protection.

Health sector data protection regulation

Four provinces have enacted specialized and comprehensive data protection statutes that govern data processing in the health care sector.[86] Only Ontario's health sector statute has been declared "substantially similar" to PIPEDA by the federal government, so it applies in place of PIPEDA for its full scope of application. In all other provinces, personal information collected, used and disclosed by health care providers in private practice is regulated by PIPEDA because they are considered to be engaged in "commercial activity."[87]

Canadian data protection legislation is not uniform, but all statutes are aimed at giving individuals control over their personal information based on "fair information practices."[88] PIPEDA, for example, requires organizations to follow ten data protection principles, including those requiring organizations to notify individuals why their information is collected, limit collection, use and disclosure, process personal information based on informed consent, be open about data protection policies and procedures and give individuals access to their personal information subject to limited and specific exceptions.[89]

Most Canadian data protection statutes contain regulation based on similar principles, though private sector legislation features informed consent as a governing principle and public sector legislation features statutory authorization as a governing principle.

---

[83] *Personal Information Protection Act*, S.B.C. 2003, c. 63 [British Columbia PIPA], *Personal Information Protection Act*, S.A. 2006, c. 25 [Alberta PIPA] and *Protection of personal information in the private sector, an Act respecting the*, R.S.Q. c. A-2.1.

[84] R.S.C. 1985, c. P-21.

[85] One notable exception: Ontario's public sector legislation has an exclusion that limits its application to employees: *Municipal Freedom of Information and Protection and Privacy Act*, R.S.O. 1990, c. M-56, s. 52(3) [Ontario MFIPPA] and *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990 c. F.31, s. 65(6) [Ontario FIPPA].

[86] *Health Information Act*, R.S.A. 2000, c. H-5 [Alberta HIA], *Health Information Protection Act*, S.S. 1999, c. H-0.021 [Saskatchewan HIPA], *Personal Health Information Act*, C.C.S.M. c. P33.5 and *Personal Health Information Protection Act*, S.0. 2004, c. 3, Sch. A.

[87] *Fact Sheet: Municipalities, Universities and Hospitals* (Ottawa: Office of the Privacy Commissioner of Canada, 2004). This means there is overlapping provincial and federal coverage of private practice health care providers in Alberta, Saskatchewan and Manitoba.

[88] A concept formalized by the Organization for Economic Cooperation and Development in its *Guidelines on the Protection of privacy and transborder flows of personal data* (Paris: OECD, 1980).

[89] PIPEDA, *supra* note 82, schedule 1.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The rights and obligations in Canadian data protection statutes apply to "personal information," which is uniformly defined as "information about an identifiable individual." This is a very broad definition which does not rest on the sensitivity of the information or an individual's expectation that the information would customarily be kept confidential.[90]

Under this definition, whether information can be used to identify an individual is an important threshold issue for the application of data privacy regulation. Most regulators will find that information which may reasonably lead to the identification of an individual based on the information alone or based on other available information is personal information. Hence, the Privacy Commissioner of Canada has held that Internet Protocol addresses are personal information.[91] The "identifiability" principle is significant to Canadian litigants who seek to protect personal privacy in producing documents by redacting personal information. It is clear that redacting names alone will not necessarily be sufficient to achieve this objective, though there is yet to be a single authoritative source that articulates the principle and its boundaries.

The basic meaning of "personal information" under Canadian data protection legislation is also subject to express and implied limitations. Most statutes will exempt "business contact information." For example, British Columbia's commercial sector and private sector employment statute expressly excludes the name, position name or title, business telephone number, business address, business email and business fax number of an individual.[92] "Work product information" – information about a person's work – is another exclusion. It is expressly excluded from the definition of personal information in British Columbia's private sector data protection statute,[93] and has also been excluded on an implicit basis, as information that is not "about" an individual.[94] Hence, the Privacy Commissioner of Canada has held that physicians' prescribing patterns are information about a professional process and not personal information about the prescribing physician.[95]

The concept of "data processing" is not strongly featured in Canadian data protection legislation. However, the types of data processing activities regulated are relatively standard, with most statutes containing rules that apply to the collection, use, disclosure, storage, retention and disposal of personal information.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

Most Canadian data protection statutes contain provisions that allow the production of documents containing a non-party's personal information to an opponent in litigation without individual consent and without providing prior or subsequent notice of disclosure. PIPEDA, for example, specifies that individual consent is not required where disclosure is, "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel

[90] The concept of sensitivity is built into the rules in Canadian data protection legislation. The standard for securing personal information, for example, varies based on the sensitivity of the information being secured. In PIPEDA, the sensitivity of personal information also goes to the required form of consent: PIPEDA, *supra* note 82, Schedule 1, principle 4.3.4.
[91] *PIPEDA Case Summary #25*.
[92] British Columbia PIPA, *supra* note 83, s. 1.
[93] *Ibid*.
[94] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 establishes that the purpose of data protection legislation does not demand inclusion of "work product information" in the definition of personal information.
[95] *PIPEDA Case Summary #14* and *PIPEDA Case Summary #15*.

the production of information, or to comply with rules of court relating to the production of records."[96] A handful of Canadian data protection statutes also contain special interpretation provisions which establish that their terms are not to be construed to limit the information available by a party to a legal proceeding.[97] The bare reference to "rules of court" in PIPEDA, without any specification that such rules must be Canadian rules, is typical in Canadian data protection statutes. This means that that Canadian parties to litigation based outside of Canada may often be able to disclose a non-party's personal information to an opponent without seeking individual consent. In every case, however, the provisions of the applicable data protection statute should be consulted.

While the production-related exemptions in Canadian data protection law facilitate production of a non-party's personal information, they only do so to the extent personal information is either required to be disclosed or reasonable to disclose. Therefore, if personal information is contained in a record that meets the "semblance of relevance" threshold for production but the personal information itself is not relevant, it would be prudent to prevent such personal information from being disclosed by either (a) redacting it completely (*e.g.,* by deleting credit card numbers), (b) redacting related identifying information (*e.g.,* by redacting credit card holders' names) or (c) by replacing identifying information with non-identifying information (*e.g.,* by replacing each credit card holder's name with a unique identifying number). Whether there is a "duty to redact" and the nature of any such duty depends on the language of the applicable data protection statute. There are strong policy arguments against a rigid duty to redact given the time and expense likely borne by parties required to engage in "personal information" document review and the costs to the system in managing disputes over redaction.[98] Nonetheless, protecting sensitive personal information in records produced in the course of litigation by taking the above-noted steps is a privacy-protective option for parties producing records that contain sensitive personal information. Moreover, it is a practice that has been endorsed by Canadian courts.[99]

Canadian data protection statutes also contain provisions that allow for the production of records containing personal information in response to third-party production orders and to law enforcement and regulatory agencies without individual consent and without providing notice of disclosure. There are three types of permissive provisions: (1) those allowing for the disclosure of personal information where "required by law" (*e.g.,* under a statutory reporting requirement or in response to a valid request made under a power of inquiry or audit); (2) those allowing for the disclosure of personal information in response to a warrant, subpoena or similar court-issued process; and (3) those giving custodians a discretion to disclose personal information to law enforcement and regulatory agencies based on a reasonable belief that the information relates to the breach of law. PIPEDA, for example, allows for disclosure without knowledge or consent if the disclosure is:

> (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
>
> (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

[96] PIPEDA, *supra* note 82, s. 7(3)(c).
[97] *See, e.g.,* Alberta PIPA, s. 4(5)(b), Ontario FIPPA, s. 64(1) and Ontario MFIPPA, s. 51(1).
[98] Note that some statutes appear to address these concerns by permitting non-consensual disclosures where "reasonable" for the "purposes of a proceeding": *See, e.g.,* British Columbia PIPA, s. 18(c) and Alberta PIPA, s. 14(d).
[99] *See, e.g., Datatreasury Corp v. Royal Bank of Canada*, [2008] F.C.J. No. 1193 at para. 19 (F.C.) (QL) and *Innovative Health Care Group Inc. v. Calgary Health Region*, [2008] A.J. No. 615 at para. 41 (C.A.) (QL).

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

(d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(iii) required by law.[100]

These PIPEDA exemptions are atypical in that they grant, with certain limitations, permission to disclose personal information to foreign governments for their own law enforcement purposes. Most other Canadian data protection statutes clearly specify that permissible disclosures are to be based on provincial or federal Canadian laws or to Canadian governments and their law enforcement agencies.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

We have addressed the implications of Canadian data protection legislation for both civil and criminal proceedings above.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Canadian data protection legislation only protects information about natural persons.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

The scope of coverage of Canadian data protection legislation is described in part (a) above. Within this scope coverage, there are certain activities which are uniformly excluded. These include journalistic activity, activity for artistic and literary purposes and personal or domestic activity.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

None.

[100] PIPEDA, *supra* note 82, s. 7(3). Section 7(3)(d) of PIPEDA was held not to violate the prohibition against unreasonable searches in section 8 of the *Canadian Charter of Rights and Freedoms* in *Royal Bank of Canada v. Welton*, [2008] O.J. No. 678 (S.C.J.) (QL). There has been significant litigation about whether the government conducts an unlawful search by seeking personal information without a warrant and through the mechanism established by section 7(3)(c.1) of PIPEDA: *See, e.g., S.C. (Re)*, [2006] O.J. No. 3745 (C.J.) (QL), *R. v. Kwok*, [2008] O.J. No. 2414 (C.J.) (QL) [Kwok] and *R. v. Ward*, [2008] O.J. No. 3116 (C.J.) (QL). This litigation, however, stresses that the question of legality is strictly about the government's right to seek personal information despite section 8 of the *Charter of Rights and Freedoms*: *See, e.g., Kwok*, *ibid.* at para. 32. There is little doubt that non-governmental custodians can disclose personal information without consent and without providing notice and comply with PIPEDA so long as the letter request meets the criteria laid out in section 7(3)(c.1). *See* generally, Suzanne Morin, "Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CAN Letter of Request Protocol", available online at http://www.cba.org/CBA/newsletters/pdf/07_08_privacy-disclosure.pdf.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

To date, Canadian courts and labour arbitrators have strongly recognized employers' right to fully control employee personal information stored on their computer systems provided they also promulgate computer use policies that clearly notify employees that they shall have no reasonable expectation of privacy.[101] While most of the case law is about the right of employers to monitor employee communications for their own purposes, it also supports the right of employers to disclose employee communications to an opponent in litigation without notice or consent.

Despite this limiting view on employee privacy, Canadian courts have nonetheless rejected claims that employees have waived solicitor-client privilege by seeking advice from their own legal counsel through an employer's communication systems.[102] This is consistent with the relatively stringent protection of solicitor-client privilege in Canadian law. It also resonates with the view expressed by some that forgiving inadvertent disclosure is particularly called for because electronically stored information is difficult to control.[103]

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

Canadian data protection legislation generally requires that individuals be given notice of the purposes for which personal information is collected and used at or before the time of collection and not prior to or subsequent to disclosure. There are a small number of exceptions. For example, the Alberta and Saskatchewan health sector statutes require custodians notify individuals of non-consensual disclosures, including non-consensual disclosures related to proceedings.[104] Likewise, the British Columbia *Freedom of Information and Protection of Privacy Act* requires a public body to notify the government of a foreign demand for disclosure.[105] Nova Scotia's public sector blocking statute, discussed further below, includes a similar requirement.[106]

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

In general, there are no special procedures that need to be followed to produce documents containing personal information for the above-noted purposes.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

Informed, individual consent is the standard embedded into most Canadian data protection legislation and no particular form of consent is required.

---

[101] *See, e.g., Lethbridge College and Lethbridge College Faculty Assn. (Bird Grievance) (Re)*, [2007] A.G.A.A. No. 67 (Ponak) (QL), *Milsom v. Corporate Computers Inc.,* [2003] A.J. No. 516 (Q.B.) (QL), *Camosun College and Canadian Union of Public Employees, Local 2081 (Re)*, [1999] B.C.C.A.A.A. No. 490 (Germaine) (QL), *International Association of Bridge, Local Union No. 97 and Structural and Ornamental Ironworkers and Office and Technical Employees Union, Local 15 (Re)*, [1997] B.C.C.A.A.A. No. 630 (Bruce) (QL) and *British Columbia and British Columbia Government Employees' Union (Bradley) (Re)*, [1995] B.C.A.A.A. No. 171 (Bird). But *see*, *University of British Columbia (Re)*, 2007 CanLII 42407 (BC I.P.C.).

[102] *See, e.g., Pacific Northwest Herb Corp. v. Thompson*, [1999] B.C.J. No. 2772 (S.C.) (QL) and *National Bank Financial Ltd. v. Potter* [2005] N.S.J. No. 186 (S.C.) (QL), aff'd, [2006] N.S.J. No. 236 (C.A.) (QL).

[103] *Eizenshtein v. Eizenshtein*, [2008] O.J. No. 2600 at para. 42 (S.C.J.) (QL).

[104] Alberta HIA, *supra* note 86, s. 42(1) and Saskatchewan HIPA, *supra* note 86, s. 21(b).

[105] R.S.B.C. 1996, c. 166, s. 30.2 [BC FIPPA].

[106] *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3, s. 61.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Canada is not a party to the Hague Evidence Convention. Instead, cross-border discovery in Canada is facilitated through international treaties, mutual agreements and the federal and provincial evidence acts.

Canada has entered into twenty-five judicial cooperation treaties whereby it provides judicial assistance to facilitate the conduct of foreign legal proceedings in civil and commercial matters.[107] In addition to the international treaties, Canada's federal and provincial statutes offer judicial assistance to foreign courts in obtaining evidence that bears relevance to their legal proceedings.

Specifically, federal and provincial evidence acts authorize Canadian courts to use their discretionary power to order the examination of a witness or the production of a document, or both, for use in foreign legal proceedings.[108] Pursuant to these provisions, a foreign litigant who is seeking relevant evidence located in Canada can submit a letter of request, also known as a letter rogatory, to a Canadian court. Provided certain criteria are met, the court will grant the letter of request. Where the criteria are not satisfied, the court may restrict the extent of the disclosure requested, and/or make it conditional upon specific undertakings.

The federal and provincial evidence acts clarify that the decision to grant or refuse a foreign discovery request is a matter of judicial discretion.

In the past, the Canadian judiciary exercised restraint in granting foreign letters of request by limiting their issuance to situations where the evidence being sought was for trial purposes, and not merely for discovery.[109] This approach appears to have been relaxed. Letters rogatory are now granted for discovery purposes, in recognition of the fact that the disclosure being sought has a natural ancillary discovery purpose that is unavoidable, and should not serve to defeat the right of the foreign petitioner to have the benefit of the testimony sought.[110]

The procedure in Quebec governing rogatory commissions is slightly different from the other provinces. Under Quebec's *Special Procedure Act,*[110] a number of procedural steps have to be followed before a foreign letters rogatory will be honoured by a Quebec court. As with the other jurisdictions, a Quebec judge has the discretionary power to enforce the letters rogatory. The disclosure request is generally allowed, unless granting the enforcement would go against Quebec public policy or public international law as it is interpreted in Quebec.

In addition to letters rogatory, Canada has passed federal legislation which facilitates international judicial co-operation in criminal legal proceedings. The *Mutual Legal Assistance in Criminal Matters*

---

[107] As of September 18, 2008, Canada is party to twenty-five bilateral and multilateral judicial co-operation treaties with the following countries: Germany, Austria, Great Britain, Northern Ireland, the United Kingdom, Iraq, Hungary, Yugoslavia, Belgium, Czechoslovakia, Denmark, Estonia, Finland, the Netherlands, Poland, Norway, Portugal, Italy, Turkey, Sweden, Spain, Austria, and France.

[108] With the exception of Prince Edward Island and Newfoundland and Labrador, all remaining Canadian provinces and territories have enacted laws authorizing judicial assistance to foreign courts. Refer to: *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 46; *Alberta Evidence Act*, R.S.A. 1980, c. A-21, s. 57; *Evidence Act*, R.S.B.C. 1996, c. 124, s. 53; *Manitoba Evidence Act*, R.S.M. 1987, c. E150, s. 82; *Saskatchewan Evidence Act*, R.S.S, 1978, c. S-16, s. 53; *Evidence Act*, R.S.O. 1990, c. E.23, s. 60; *Evidence Act*, R.S.Y.T. 1986, c. 57, s. 63; *Evidence Act*, R.S.N.W.T. 1988, c. E.8, s. 72; *Special Procedures Act*, R.S.Q., ch. P-27, ss. 9-20.

[109] Editors of American Bar Association, eds., *Obtaining Discovery Abroad*, 2d ed. (Chicago, Illinois: American Bar Association, 2005) at 83 [Obtaining Discovery Abroad].

[110] *Henry Bacon Building Materials Inc. v. Royal Canadian Mounted Police* (1994), 98 B.C.L.R. (2d) 59 (S.C.), *GST Telecommunications Inc. v. Provenzano* (2000), 73 B.C.L.R. (3d) 133 (S.C.).

[111] R.S.Q. c. P-27.

Act[112] grants Canadian courts the power to issue compulsory measures, such as evidence gathering orders and search warrants, to obtain evidence in Canada on behalf of a foreign state for use in a criminal investigation and prosecution being conducted by that state. The legislation only implements requests made by a foreign state pursuant to a bilateral or multilateral treaty, or by designation under the Act.

Under the *Mutual Legal Assistance in Criminal Matters Act,* the United States and Canada have entered into a treaty which determines the nature and scope of, and the conditions for, investigative and legal assistance between Canada and the United States.[113] Pursuant to this treaty, if U.S. authorities want to obtain personal information held by the federal or provincial government or by a company or an individual in Canada, the usual course of action is to make a request to the Government of Canada. Canada's federal Department of Justice may then apply to a court in Canada for a search warrant to compel the disclosure of the information sought. Once the information is obtained, the Department of Justice will transmit the information to the United States government.

Canada and the United States are also parties to an Agreement Regarding the Application of Their Competition and Deceptive Marketing Practices Laws.[114] This agreement facilities cross-border discovery by promoting cooperation and coordination between the U.S. and Canadian competition authorities.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

Canada has legislated a number of blocking statutes. While the Supreme Court of Canada has acknowledged that blocking statutes serve the important purpose of preserving national sovereignty, the Court has also cautioned that these statutes "impede successful litigation" by refusing recognition and compliance of foreign orders.[115] To this end, the Court has emphasized that blocking statutes run counter to comity and "discourage international commerce and efficient allocation and conduct of litigation."[116]

The federal *Foreign Extraterritorial Measures Act*[117] creates a number of mechanisms to permit the Canadian government to counteract the extraterritorial application of foreign laws where they potentially infringe upon Canadian sovereignty. Section 3 of *Foreign Extraterritorial Measures Act* permits the Attorney General of Canada to make orders restricting or prohibiting the production of records where there are concerns that a foreign tribunal is exercising, has proposed to exercise, or is likely to exercise its jurisdiction in a manner that would adversely impact Canadian interests, or otherwise jeopardize Canadian sovereignty.

Presently, only one order has been issued under the *Foreign Extraterritorial Measures Act*. This is the *Foreign Extraterritorial Measures (United States) Order*,[118] which was enacted in response to the passage of the Cuban Assets Control Regulations in the United States. Under this Order, the Attorney General of Canada has the authority to monitor any extraterritorial measures from the United States that may have an adverse impact on trade or commerce between Canada and Cuba.

There are very few cases where the *Foreign Extraterritorial Measures Act* has been employed to block a foreign discovery request. In one instance, the Act was used to limit the scope of a foreign request,

[112] R.S.C. 1985, c. 30. http://www.justice.gc.ca/eng/dept-min/pub/fps-sfp/fpd/ch43.html.
[113] *Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters*, United States and Canada, 24 January 1990, Can. T.S. 1990 No. 19, 100th Cong., 2nd Sess. Exec. Rept. 100-28.
[114] 1995 Can. T.S. No. 15.
[115] *Hunt v. T&N plc*, [1993] 4 S.C.R. 289 at para. 61 [*Hunt*].
[116] *Id.* at para. 61.
[117] R.S.C. 1985, c. F-29.
[118] 1992, S.O.R./92-584.

which originated from litigation involving a contravention of U.S. laws that criminalized trading with Cuba.[119] The U.S. law was in direct opposition to Canadian public policy, which had been developed to explicitly safeguard trading between Canada and Cuba. The court criticized the foreign discovery request, which it interpreted as a failure of American authorities to comply with accepted international conventions related to comity of nations.[120] Instead of denying the request in its entirety, the court sought the assistance of the litigating parties to restrict and confine the scope of the discovery.

In addition to the federal statute, Quebec has enacted the *Business Concerns Records Act.*[121] This legislation serves as a blocking statute, and was expressly enacted in defence to the extraterritorial reach of United States anti-trust legislation, and to safeguard against other foreign judicial interference.[122] The *Business Concerns Records Act* prohibits the removal from Quebec of "documents of business concerns in Quebec that are required pursuant to judicial processes outside the province."[123] The Act is viewed as remedial legislation designed to protect Quebec companies from perceived abuses under American discovery procedures in antitrust matters. Accordingly, the Act is widely drafted and has been liberally interpreted.

The Supreme Court of Canada has held that the *Business Concerns Records Act* is not applicable, on constitutional grounds, between Canadian provinces.[124] However, the Act continues to apply with respect to demands for business-related documents from foreign courts. The *Business Concerns Records Act* does not confer immunity upon a witness, unless the entire examination conflicts with the Act; nonetheless, the Act is effective in restricting the scope of the evidence that can be gathered.

The majority of cases involving the application of the *Business Concerns Records Act* arise in the context of disclosure to other Canadian provinces. In one instance relating to a foreign disclosure request, the litigant submitted a letter rogatory to compel the production of certain business documents, disclosure of which was not permitted under the *Business Concerns Records Act.*[125] The foreign litigant challenged the application of the Act to the disclosure on the grounds that the Act was inconsistent with international law and obsolete. The court quashed the documentary request sought because it contravened the *Business Concerns Records Act.* The court also disregarded the constitutional argument, noting that the Act had existed alongside the *Special Procedure Act* for over 50 years and could only be modified through legislative intervention.

In conjunction with Quebec, Ontario has also enacted the *Business Records Protection Act,*[126] a blocking statute designed to prevent business records from being taken or sent outside of Ontario, except in specific circumstances where the transfer is legally allowed. The Ontario statute was likewise enacted in response to what was perceived to be the "aggressively extraterritorial, 'long arm'" of U.S. legislation.[127]

There have been a couple of attempts to use the *Business Records Protection Act* to block documentary disclosure pursuant to a foreign letter of request.[128] Both cases concerned criminal charges that had

[119] *Morgan, Lewis & Bockius LLP v. Gauthier*, [2006] O.J. No. 4936 (S.C.J.) (QL) [*Gauthier*].
[120] *Id*.
[121] R.S.Q. c. D-12.
[122] *Hunt*, s*upra* note 115, at para. 18.
[123] *Id.*
[124] *Id.*
[125] *Southern New England Telephone Company c. Zrihen*, [2007] Q.J. No. 2595 (S.C.) (QL).
[126] R.S.O. 1990, c. B.19.
[127] *Hunt*, s*upra* note 115, at para. 62.
[128] *France (Republic) v. De Havilland Aircraft of Canada Ltd*., [1991] O.J. No. 1038 (S.C.J.) (QL); *Germany (Federal Republic) v. Canadian Imperial Bank of Commerce*, [1997] O.J. No. 70 (S.C.J.) (QL).

been laid in a foreign court, and required disclosure of relevant evidence in Canada pursuant to section 46 of the *Canada Evidence Act*. Despite the fact that some of the information sought pertained to business records, the court rejected the argument that disclosure could be avoided due to contravention of the *Business Records Protection Act*. The court noted that the documentary disclosure being sought engaged section 46 of the *Canada Evidence Act*; therefore, this likely triggered the exception in the *Business Records Protection Act* which mandates disclosure pursuant to a subpoena or order from the Parliament of Canada.[129]

In addition to the above, two provinces, Nova Scotia and British Columbia, have enacted privacy legislation with blocking provisions that apply to disclosure sought from certain public bodies in those provinces. Under the Nova Scotia *Personal Information International Disclosure Protection Act,*[130] public bodies and municipalities are required to ensure that any personal information held by them remains in Canada, and is accessed and disclosed only in Canada, unless exceptional circumstances arise. Similarly, the British Columbia *Freedom of Information and Protection of Privacy Act*[131] requires a public body to notify the government of a foreign demand for disclosure. The public body can also refuse the disclosure where there are concerns that the disclosure may be harmful to a law enforcement matter,[132] intergovernmental relations or negotiations,[133] individual or public safety[134] or the personal privacy of third parties.[135]

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

A Canadian court will apply four preconditions in deciding whether to enforce a foreign letter of request:

- It must appear that a foreign court is desirous of obtaining the evidence.
- The witness whose evidence is sought or the document being sought must be within the jurisdiction of the court which is asked to make the order.
- The evidence sought must be in relation to a civil, commercial or criminal matter that is pending before a foreign court.
- The foreign court must be a court of competent jurisdiction, such that the court seeking the letters enforcement must have the power to grant the relief sought within its own jurisdiction.[136]

If these criteria are met, a Canadian court will then exercise a discretion based on a consideration of six factors: relevance, necessity, specificity, availability, measure of burden and consistency with Canadian public policy.

Relevance

The requested evidence must be relevant to the foreign action. Specifically, the disclosure request must identify the facts that establish the relevance of the evidence to the foreign action. With respect to this, courts have held that potential relevance is not enough; rather, the evidence

[129] *Id.*
[130] S.N.S. 2006, c. 3.
[131] R.S.B.C. 1996, c. 165.
[132] *Id.* at s. 15(1).
[133] *Id.* at s. 16(1).
[134] *Id.* at s. 19(1).
[135] *Id.* at s. 22(1).
[136] *France (Republic) v. De Havilland Aircraft of Canada Ltd.* (1991), 3 O.R. (3d) 705 at 710 (S.C.J.).

sought has to be identified with a degree of specificity and must be necessary, in order to avoid a fishing expedition.[137]

Necessity

The evidence must be necessary for pre-trial discovery or trial of the foreign action.

Specificity

The documents sought must be identified with reasonable specificity. Canadian courts have consistently held that broad and general disclosure requests are not likely to succeed; at the very least, the requested documents should be specifically described by class.[137] Overly broad and vague disclosure requests are not permitted because the courts consider this as oppressive to those called upon to produce the documents.[139]

Availability

The evidence sought must not be otherwise obtainable. Canadian courts have held that letters of request must specifically demonstrate that the requested evidence is not otherwise available, as opposed to merely asserting the same.

Measure of Burden

The request for disclosure must not be unduly burdensome. The scope of the request is measured against what the party's obligations would be if the litigation were conducted in Canada.[140] This requirement serves to shield non-parties from being subject to examination in a manner that could be "potentially intrusive, costly and time-consuming."[141]

Canadian Public Policy

The order sought must not be contrary to Canadian public policy. For example, courts will not permit a request for disclosure where there is a risk of self-incrimination by a proposed witness.[142] Canadian courts have consistently held that the risk of self-incrimination violates a principle of fundamental justice under the Charter, and contravenes Canadian public policy. In order to minimize this risk, courts may permit the disclosure being sought, subject to specific undertakings that protect the individual who is being compelled to testify or produce documentary evidence.[143]

In relation to Canada and the United States, Canadian courts will disallow discovery requests on grounds of public policy where the litigation relates to U.S. law that contravenes Canadian law. For instance, where a disclosure request was made pursuant to U.S. law that precluded trading with Cuba, the Ontario court held that the U.S. enactment was in direct contravention to Canadian public policy.[144] The court further noted that Canada had passed specific legislation which explicitly prohibited compliance with the United States measures prohibiting trade with Cuba.

[137] *Presbyterian Church of Sudan v. Rybiak*, [2005] O.J. No. 3212 (S.C.J.) (QL).
[138] *National Telefirm Assocs., Inc. v. United Artists Corp.*, [1958] 14 D.L.R. (2d) 343, 348 (Ont. H. Ct.).
[139] *Ibid.*
[140] *Advance/Newhouse Partnership v. Brighthouse Inc.*, [2005] O.J. No.566 (S.C.J.) (QL).
[141] *Ontario (Attorney General) v. Stavro* (1995), 26 O.R. (3d) 39.
[142] *EchoStar Satellite Corp. v. Quinn*, [2007] B.C.J. No. 1799 at para. 57 (S.C.) (QL).
[143] *Ibid.* at para. 62.
[144] *Gauthier*, *supra* note 119.

With respect to oral testimony, the criteria for granting a request will require demonstrating that: (1) the testimony sought is expected to bear on the issues in the action; (2) the Canadian court's assistance is not frivolously sought nor is used as a device for harassment; (3) the testimony cannot reasonably be obtained without the assistance of the Canadian court, and (4) the means available through the requesting court are inadequate to procure the attendance of the witness.[145]

[145] Obtaining Discovery Abroad, *supra* note 109, at 88

France

Christian Bouckaert **- *Lead Editor***
Bernard Mettetal **- *Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

France is a civil code jurisdiction, in which, however, many rules are created by case law.

Leaving aside the Constitutional Court, which deals solely with constitutional matters, France has a dual system of courts, consisting of two separate *ordres*, or hierarchies: the *ordre judiciaire* (for private law) and the *ordre administratif* (for public law). In the rare cases where it is unclear whether a case should be heard before an ordinary court or an administrative court, the decision is referred to a special court, the *Tribunal des conflits*.

The *ordre judiciaire*

The courts of the *ordre judiciaire* are the ordinary (civil and criminal) courts, which have jurisdiction over cases that do not involve the state, a state employee or a public body and which primarily apply private law. They are organized and function pursuant to the provisions of the Code of Judicial Organization (*Code de l'organisation judiciaire*) and the Code of Civil Procedure (*Code de Procédure Civile* – CPC).

The Cour de Cassation is the highest civil and criminal court. It has six divisions: three civil divisions (called the First, Second and Third *chambres civiles*), one Industrial Relations Division (*chambre sociale*), one Commercial Division (*chambre commerciale*) and one Criminal Division (*chambre criminelle*).

The trial courts of the *ordre judiciaire* are organized in a two-tier system: (i) the courts of first instance, and (ii) the appellate courts, which conduct a de novo examination of the whole case, both as to the facts and as to the law.

Civil litigation brought in the courts of France is governed by the rules established principally in the Civil Code and the CPC.

There is no rule of binding precedent as such, but there is a well-established practice that the trial courts of the *ordre judiciaire* will normally follow the decisions of the Cour de Cassation.

The *ordre administratif*

The courts of the *ordre administratif* have jurisdiction over administrative disputes and primarily apply public law.

The administrative courts are organized and operate under the rules established in the Code of Administrative Justice (*Code de justice administrative*).

The Conseil d'Etat – or, more precisely, the Litigation Division (*section contentieuse*) thereof – is the supreme administrative court. (The Conseil d'Etat has five other divisions, which are purely administrative in nature in that they advise the government on bills and draft decrees and their potential legal implications.)

The decisions of the Conseil d'Etat are, in practice, binding on the courts of first instance (*tribunaux administratifs)* and appellate courts (*cours administratives d'appel)* of the *ordre administratif*.

Rules of evidence in civil/commercial litigation

The law of evidence, which encompasses the law relating to disclosure, is codified in the CPC and Civil Code and supplemented by many judge-made rules.

The CPC deals with the general principles governing trials (Arts. 9-11 and 15-17) and a large part of the rules of evidence (Arts.132-322), while the Civil Code deals with the different means of proof (Arts. 1315-1369).

In civil matters, the French evidentiary system distinguishes between proof of facts and proof of legal transactions. Facts can be proved by any means, whereas legal transactions involving an amount of €800 or more must be proved - at least partially - in writing (Civil Code Art. 1341).

In commercial matters, both facts and legal transactions can be proved by any means (Commercial Code Art. L.110-3).

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

Evidence in support of a party's contentions

According to the French civil procedural principal of adversarial proceedings, the parties to a lawsuit must clearly and fully set forth their factual and legal arguments in their briefs. Pursuant to Article 15 of the CPC, the parties must, in due time, disclose to each other all the facts, points of law and items of evidence (including electronic evidence) upon which they rely, so that each party is in a position to prepare his/her answer or reply.

The parties must further spontaneously disclose to each other all documents referred to in their respective briefs (CPC Art. 132: "The party who refers to a document is required to disclose it to the other party to the proceeding. Disclosure must be spontaneous").

The same obligation is also enshrined in the national Rules of Professional Conduct of the French Bar (*Règlement Intérieur National*), Rule 5 of which requires counsel to make spontaneous, full reciprocal disclosure of evidence and factual and legal arguments in a timely manner and by the methods prescribed in the rules of procedure.

The court will set a timetable for the case, usually at a case-management conference (CPC Arts. 757 *et seq*.). The claimant may file a reply and adduce additional documents in response to the defendant's answer, and the defendant may file a rejoinder and adduce additional documents in response to the claimant's reply. Additional documents and new legal contentions (but not new claims) may be introduced on appeal.

Finally, evidence obtained by unlawful means may not be used in court (*see*, *e.g.*, Cour de Cassation, Industrial Relations Division, Nov. 20, 1991, D. 1992, jurispr. 73, which ruled inadmissible tapes of employees' conversations recorded without the employees' knowledge).

If documents referred to in a party's pleadings have not been disclosed spontaneously and in due time, the other party may, without formality, request the court to issue an order for their disclosure (CPC Art. 133). In making such an order, the court will set a time limit for disclosing the documents in question, if necessary on penalty of

a daily fine, and, where applicable, specify the manner in which they are to be disclosed (CPC Art. 134). The court may exclude from the hearing those documents which have not been disclosed in due time (CPC Art. 135).

Evidence detrimental to a party's contentions

The main principle of the French rules of evidence is that a party has no duty to disclose spontaneously any documentary or other evidence that does not support his contentions. This may be seen as the extreme consequence of the freedom accorded to the parties by the adversarial principle.

However, pursuant to the second paragraph of Article 11 of the CPC, if a party withholds an item of evidence, even one not referred to the party's pleadings, the other party may request the court to issue an order for its disclosure, if necessary on penalty of a daily fine. The preconditions for the issuance of such an order are that the evidence sought must be sufficiently identified and in the possession of the other party, and there must be no legal reasons preventing its disclosure (*e.g.*, professional secrecy, or right to respect for private life and correspondence).

The court has discretion to decide whether to compel a party to produce a piece of evidence. The court will issue a disclosure order only if it is satisfied that the evidence sought is necessary to provide the court with a clearer picture of the case and is material to the court's determination.

On the international side, it should be noted that France entered a reservation under Article 23 of The Hague Convention of March 18, 1970, on the Taking of Evidence Abroad in Civil and Commercial Matters. Accordingly, France will not execute "letters of request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries."

Since 1989, the reservation does not apply when the letter of request seeks to obtain the production of specified documents directly related to the pending action. Still, the basic purpose of the reservation is to prevent "fishing expeditions".

There are, however, some attenuations to the above principle. The CPC prescribes specific rules for pre-trial gathering of evidence in, *e.g.,* trademark-infringement or unfair-competition cases. More broadly, Article 145 of the CPC provides for a separate judicial procedure to preserve and evaluate evidence under certain circumstances. Article 145 permits potential future litigants to obtain evidence likely to be material to the resolution a dispute:

> If, before any proceedings have been commenced, there is good cause to preserve or establish proof of facts upon which the outcome of the dispute may depend, legally permissible evidence-taking measures may be ordered at the request of any interested party, by way of a petition or a summary procedure.

Within the framework of evidence-taking measures under Article 145, French judges often appoint court-certified experts (*experts judiciaires*), who are independent, recognized specialists in their field and whose role is to help the judges decide cases involving questions of fact that require specialist knowledge. The surveys and/or investigations conducted by such experts (*expertises judiciaires*) and the ensuing reports issued by them (*rapports d'expertise*) play an essential role in most litigation under French procedural law. One or more experts are appointed and assigned their tasks by a specific order issued by the judge after hearing the arguments of the potential litigants and considering their suggestions for the wording of the terms of reference. The appointed expert(s) must explicitly accept their terms of reference and fulfill them conscientiously and impartially.

One of the tasks usually assigned to court-appointed experts is to inspect all documents necessary to fulfill their terms of reference. This allows the court-appointed experts to require the parties to hand over whatever documents they deem necessary for that purpose. If a party fails or refuses to do so, the expert may move the court for an order directing the party to produce specified documents, if necessary on penalty on a daily fine. The court will decide whether the documents sought are relevant under the circumstances of the case. Also, the court may draw negative inferences from a party's failure or refusal to produce requested documents (CPC Art. 11-1).

In a perfect world, the expert opinion would enlighten the court on the technical aspects of the case and enable the court to make the appropriate findings of fact and conclusions of law.

Courts are not bound by the expert opinions they order, but in most cases they will accept them as conclusive evidence of the technical facts in issue. Expert opinions therefore play a significant role in, and influence the outcome of, legal proceedings.

In modern litigation, Article 145 CPC is no doubt the best way under French law to obtain documents that would not be spontaneously produced in the absence of a court-ordered expert opinion.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Disclosure from a non-party may be obtained prior to the institution and/or during the course of proceedings.

The court may, on the motion of one of the parties, request or order, if necessary on pain of the same penalty [a daily fine], the production of all documents in the possession of third parties, provided that there are no legal reasons preventing their production (CPC Article 11-2).

If, in the course of the proceedings, a party wishes to rely on a notarial deed or private contract to which he was not a party or a document held by a third party, he may request the court seized of the proceedings to order the production of a certified copy or the original of the deed, contract or document (CPC Art. 138).

Here too, the court has discretion in deciding whether to issue a disclosure order and whether to make it subject to a daily fine for non-compliance. In exercising its discretion, the court may need to weigh the legitimate interests of the movant against the legitimate interests of the third party (professional or medical secrecy, right to respect for private life, etc.), which could be violated by granting the motion for a disclosure order.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

Under French law, there are no specific provisions requiring a party or potential party to preserve documents for the purpose of civil proceedings. But any party or non-party that has been ordered by the court to disclose documents is under the implicit obligation to preserve the documents in question.

Although there are no specific rules relating to the preservation of documents for the purpose of civil proceedings, the codes do contain various obligations to preserve documents for other purposes. For example, Article 123-22 of the Commercial Code requires businesses to keep accounting records and supporting documents for 10 years.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

   As there is no general rule in the CPC regarding the preservation of documents for the purpose of civil proceedings, there are no general codified sanctions either. The court may, however, award damages against a party proved to have knowingly destroyed documents relevant to pending or potential litigation.

   Also, the civil courts have discretion with respect to documents that have gone missing or are otherwise no longer available. The court may, for instance, shift the burden of proof. Furthermore, a litigant who has produced and later suppresses or withdraws a title deed, an exhibit or a memorial is liable to a fine under Article R.645-7 of the Penal Code.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

   There is no specific rule concerning the costs of discovery/disclosure.

   In the rare cases where discovery/disclosure costs could be individualized and quantified, they would be included in the general costs borne by the losing party according to Article 700 of the CPC:

   > In all proceedings, the court shall order the party bearing the burden of the taxable costs or, in default, the unsuccessful party, to pay to the other party such amount as the court shall fix on the basis of the sums expended and not included in the taxable costs. The court must take into consideration the rules of equity and the financial circumstances of the party ordered to pay. The court may, on its own motion, for reasons based on the same considerations, rule that there is no need for such order.

   The court may find it equitable to require the losing party to pay a portion of the successful party's legal expenses (including attorneys' fees). In practice, the amounts awarded by French courts in this respect are modest, if not nominal.

   Special mention should be made here of expert opinions ordered under Article 145 CPC. The costs of an expert opinion (fees and expenses of the court-appointed expert(s), charges for lab analyses and studies by research centers, etc.) may be high. Typically, the court will order the claimant to advance said costs, and ultimately award them against the losing party.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

   Since French law has not established an obligation of disclosure in civil proceedings, there are no specific rules concerning electronic disclosure. The Civil Code does, however, contain a few provisions relating to electronic documents.

   Electronic documents have been treated just like any other documents since the law of March 13, 2000, which transposed European Directive 1999/93/EC into French law.

   As a matter of fact, the above-mentioned law specifies that the term "documents" is not confined to paper writings but extends to electronic records. The law further specifies that electronic documents are admissible as evidence, provided that their author can be identified and that they have been prepared and stored in conditions calculated to secure their integrity (Civil Code Arts. 1316-1 to 1316-3).

A subsequent law of June 21, 2004, codified as Article 1108-1 of the Civil Code, provides that whenever the law requires that a contract be reduced to writing, the requirement may be satisfied by an electronic document, except in family, inheritance or suretyship matters.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   There are no provisions in the CPC and no case law defining electronic documents for disclosure purposes.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

   There are no legal provisions or rules (in place or proposed) in France that require the parties to meet and discuss electronic disclosure. Should the need arise, the parties would probably discuss electronic disclosure at a case-management conference.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

    There are no legal provisions or rules (in place or proposed) in France that require parties to preserve electronic documents related to pending or possible future litigation, other than the provisions and rules governing disclosure in general set forth in Part One hereof.

    There are, however, some specific obligations to preserve electronic documents outside the context of pending or possible future litigation. As previously stated, Article 123-22 of the Commercial Code establishes a general obligation for businesses to keep accounting records for 10 years. Given that electronic records are treated in the same way as paper records, the obligation should be construed as applying to electronic accounting documents too.

    The law of June 21, 2004 and the decree of March 24, 2006 require Internet-service and web-hosting providers to keep connection records for a year and to transmit them to judicial authorities on request. Pursuant to Article L.134-2 of the Consumer Code and to Decree 2005-137 of April 16, 2005, businesses must keep records for 10 years of all electronic transactions involving an amount greater than €120.

    There is nothing, however, in the law that specifies how electronic documents are to be preserved. Article 1316-1 of the Civil Code merely requires that they be "stored in conditions calculated to secure their integrity."

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

    A general legal obligation to search for, disclose and produce documents is alien to French procedural laws, and this applies to electronic documents as well.

    Nothing, however, prevents a party from seeking an order under Art. 145 CPC for disclosure by another party of limited and pertinent information stored in servers or computers, provided that the information is likely to be material to the outcome of the dispute and is not covered by attorney-client or medical privilege or any other legal impediment to its disclosure.

    Under such circumstances, the judge will impose restrictions on the search for, and production of, the information. The judge will not entertain a fishing expedition, or even a motion for an order for general disclosure of all the commercial correspondence, whether via e-mail or other media.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

    No such provisions or rules exist in French law.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

    No specific provisions or rules exist in French law. Should the issue arise, it would be dealt with in the judge's order.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

    French law has set no legal standard specific to electronic information. However, Article 9 of the CPC provides that evidence must be adduced in accordance with the law: "Each party must prove, according to the law, the facts necessary for the success of his claim."

    Since electronic documents are now treated like any other documents by French law, they are subject to the above provision. Consequently, electronic documents obtained fraudulently or in a manner contrary to public order are not admissible in evidence. The same applies to documents constituting an invasion of privacy, such as those covered by professional secrecy or pre-trial investigation secrecy. Invasion of privacy may be characterized by the disclosure of correspondence, medical records or tax returns. This principle includes a duty to act fairly, under which any recording, filming or tailing of a person without his or her knowledge is unlawful.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

    Since there is no obligation of en masse disclosure/production, the question of the treatment of inadvertently disclosed privileged information does not arise.

    That being said, there is a legal privilege for attorney-client communications.

    Rule 2 of the *Règlement Intérieur National* (Rules of Professional Conduct of the French Bar) states that the attorney-client privilege includes all confidential disclosures made by the client, as well as all facts and documents received by the attorneys in their capacity as such.

    An attorney who violates the privilege is liable to disciplinary sanctions ranging from a reprimand to disbarment, depending on the seriousness of the violation, and also to criminal penalties under Article 226-13 of the Penal Code (for breach of professional secrecy).

    Save two very limited exceptions, Rule 3 of the *Règlement Intérieur National* forbids attorneys to produce in court any notes or communications received from attorneys acting for the other side.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

    There is no specific rule concerning the costs of e-discovery/e-disclosure.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

    Such policies and procedures are used only by some French firms doing business in the United States.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

    Not at all.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    There are two sets of rules under French law that impact on the disclosure/production of documents.

    - The first set of rules is the previously mentioned 1978 Data Protection Act, as amended by the law of August 6, 2004, containing provisions regarding the movement of personal data to third countries.

      The 1978 Act, as amended, establishes the principle of free and unrestricted cross-border flows of personal data within the European Union.

      Article 68 of the 1978 Act, as amended, provides that data transfers outside the EU are not permitted unless the receiving country ensures an "adequate level of protection."

      The "adequate level of protection" is assessed in accordance with the purpose and duration of the proposed processing operation or operations, with the rules of law, both general and sectoral, in force in the third country in question and with the professional rules and security measures that are complied with in that country.

      However, according to Article 69, a transfer of personal data to a third country that does not ensure an adequate level of protection may take place if the data subject has unambiguously given his or her consent to the transfer, or if the transfer is:

        - necessary in order to protect the vital interests of the data subject; or
        - necessary [or legally required] on important public interest grounds; or
        - necessary [or legally required] for the establishment, exercise or defense of legal claims; or
        - made from a register that is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate legitimate interest; or
        - necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
        - necessary for the conclusion or performance of a contract concluded or to be concluded in the interest of the data subject between the controller and a third party.

    - The second set of rules is the law of July 16, 1980, on the taking of evidence in view of legal or administrative proceedings abroad.

      The provisions of that law, which is sometimes referred to as "the French Blocking Statute," will be addressed below (IV.14(b)).

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

The ever-more widespread use of computers created the need both to facilitate free movement of einformation and to protect fundamental freedoms, in particular the right to privacy. An open net is a ready source of exploitable data on Internet users. That is why each individual must be protected against misuse of any personal data he or she may have left on the Web. The concern about misuse, especially by government agencies, of information technology increased at the end of the 1960s. The aim at that time was to protect individuals against misuse of their personal data held by government agencies and to grant them direct access to such data.

The 1978 French Data Protection Act (Law No. 78-17 of January 6, 1978) stems from the *Safari* scandal. In the 1970s, the French Government was developing a computer system, called Safari (*Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*), whereby all data held by government agencies on a given individual could be called up by entering a single identification number.

The disclosure of the Safari project sparked a huge scandal in France, forcing the government to create the "Information and Freedom Commission" and resulting in the 1978 Data Protection Act (the "1978 Act").

The 1978 Act endeavors to reconcile the rights of individuals and the freedom to collect data on individuals. It does not prohibit the creation of personal files. Its main purpose is simply to regulate the utilization of information technology.

The 1978 Act was amended by Law No. 2004-801 of August 6, 2004, when France transposed Directive 95/46/EC of the European Parliament and of the Council, of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "1995 Directive").

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

"Personal data" and "processing of personal data" are defined in Articles 2(2) and 2(3) of the 1978 Act, as amended.

> Art. 2(2): Personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him.
>
> Art. 2(3): Processing of personal data shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

See answer to question 19 above.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

The scope of the 1978 Act, as amended, is wider than that of the 1995 Directive. The Act applies to processing operations concerning, *inter alia*, public security, defense, State security and the activities of the state in the area of criminal law.

There is no specific provision concerning civil or criminal proceedings, except Article 10 of the 1978 Act, as amended, which states that:

- no court decision involving the assessment of a subject's behavior may be made solely on the basis of electronic personal data intended to assess some aspect of the subject's personality, and
- no court decision may be made solely on the basis of electronic personal data intended to define the subject's profile or some aspect of his personality.

Moreover, pursuant to Article 8, the collection and processing of sensitive data, usually forbidden, are allowed if necessary for the establishment, exercise or defense of legal claims.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Several rights are accorded to data subjects:

Right to prior information (Art. 32 of the 1978 Act, as amended)

The controller must inform every data subject about the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.

Right of access to data (Art. 39 of the 1978 Act, as amended)

Every data subject has the right to obtain from the controller all data relating to him.

This right accrues solely to natural persons and to the managers of legal persons whose names are listed in the file.

Right to query (Art. 39 of the 1978 Act, as amended)

The controller must confirm to the data subject, on request, whether or not data relating to him are being processed.

Right of communication (Art. 39 of the 1978 Act, as amended)

The data subject has the right to obtain communication of the data undergoing processing and of any available information as to their source.

Right of rectification (Art. 40 of the 1978 Act, as amended)

The data subject has the right to obtain from the controller the rectification, erasure or blocking of data that are incomplete, inaccurate, ambiguous or out-of-date or whose collection, communication, use or preservation is forbidden.

Right to object (Art. 38 of the 1978 Act, as amended)

The data subject has the right to object on legitimate grounds to the processing of data relating to him, unless said processing is a legal obligation.

The data subject may also object, on request and free of charge, to the processing of personal data relating to him that the controller anticipates being processed for the purposes of direct marketing.

Right to oblivion – (Art. 6, para. 5, of the 1978 Act, as amended)

Data must not be retained any longer than necessary to achieve the purpose for which they are collected and processed, such as data relating to children or teenagers.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

French data protection and privacy legislation does not apply to automatic processing of personal data in the course of a purely personal activity (Article 2 of the 1978 Act, as amended).

Nor does said legislation apply to temporary copies made within the context of technical activities of transfer and supply of access to a digital network, with a view to automatic intermediary and temporary storage of data and for the sole purpose of providing other receivers of the service with the best access to transmitted data (Article 4 of the same Act).

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

Article 8 of the 1978 Act, as amended, lists sensitive personal data whose collection and processing are forbidden.

The data in question are those which reveal, directly or indirectly, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

However, some exceptions are allowed subject to certain conditions. These exceptions, listed at Article 8, are as follows:

1. Processing to which the subject data has given his explicit consent, except where the law provides that the prohibition may not be lifted by the data subject's giving his consent;
2. Processing necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving his consent;
3. Processing carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely

to the members of the body or to persons who have particular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

4. Processing relating to data that are manifestly made public by the data subject;
5. Processing relating to data that are necessary for the establishment, exercise or defense of legal claims;
6. Processing required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional or other person subject to the obligation of professional secrecy;
7. Processing of data carried out by the INSEE (French National Institute of Economic and Statistical Information) or by the statistics department of a ministry;
8. Processing necessary for health research;
9. Processing of anonymous data;
10. Processing justified by public interest.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

In 2001, the French Supreme Court (Cour de Cassation) had to deal with employer monitoring of employees' personal e-mails. In *Nikon France SA v. Frédéric Onos*[146] (October 2, 2001), the Court said that employees have a right to privacy of correspondence in the workplace. The court held that evidence collected by the employer from files of e-mails stored in the company's computer hard drive, showing that the employee was doing freelance work during office hours, was a breach of privacy.

Employers do not have the right to access their employee's personal emails unless the principle of proportionality is respected. This means that the monitoring, and the sanctions imposed, by the employer must be proportionate to the objective pursued.

In a 2005 case,[147] the French Supreme Court held that an employer cannot open files identified as personal on the office computer used by an employee unless the employee is present. In this case, the employer, after finding erotic pictures in the drawer of an employee's desk, checked the employee's computer and discovered various documents unconnected with the employee's duties, whereupon the employer discharged the employee. The Court ruled the discharge unfair because the search of personal data outside the employee's presence was not justified by a particular risk or event.

An employee's electronic data are presumed to be business related unless otherwise specified by the employee. Employer monitoring is still allowed but limited to specific circumstances.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

Before its amendment in 2004, the 1978 Act required controllers to notify the supervisory authority before carrying out any wholly or partly automatic processing operation.

[146] Bull. Civ.V, 2001 No. 291.
[147] Cass. Soc., May 17, 2005, Juris-Data No. 2005-028449.

The Act made a distinction between the public and private sectors. Processing by organizations in the public sector was subject to notification to, and prior authorization from, the regulating agency, whereas processing by organizations in the private sector was merely subject to notification.

Account was also taken of the sensitive nature of the data collected.

Now, under Article 22 of the 1978 Act, as amended, only processing presenting particular risks to rights and freedoms is subject to notification to, or authorization from, the French regulating agency.

Article 32 of the Act lists the information to be provided to the data subject, namely, the identity of the controller and of his representative, if any; the purposes of the processing for which the data are intended; whether replies to the questions are obligatory or voluntary, and the possible consequences of failure to reply; the recipients or categories of recipients of the data; the existence of the right of access to and the right to rectify the data concerning him; and whether the data is intended to be transferred to third countries.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

No such procedures have been established by the 1978 Act, as amended.

However, Article 99-3 of the Code of Criminal Procedure provides:

> An investigating judge or a police officer commissioned by an investigating judge may request any person, any public or private establishment or organization or any government agency likely to hold documents of interest to the investigation, including those issuing from a registered computer or data-processing system, to hand over such documents to him, including in digital format. The obligation of professional secrecy may not, without good cause, be given as a reason for not complying with the request.

Documents requested of lawyers, notaries, bailiffs, doctors or publishing or media and communications companies may not be handed over without their consent.

Any individual or entity – other than those mentioned above – that refuses to comply, or fails to comply promptly, with such a request is liable to a fine of €3,570.

Moreover, Article 99-4 of the Code of Criminal Procedure provides that a police officer commissioned by an investigating judge may, with explicit authorization from the latter, issue the requests provided for in the second paragraph of Article 60-2, namely, requests to telecommunications operators to take, without delay, all measures conducive to preserving, for a period not exceeding one year, the content of information consulted by users of the services provided by the operators.

Any operator that refuses, without good cause, to comply with such a request is liable to a fine of €3,570.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

The 1978 Act contains no specific provision concerning employee consent for the processing and transfer of personal data.

However, Article 7 of said Act provides that the processing of personal data must be carried out with the consent of the data subject or be necessary for certain specified purposes, *e.g.*, legitimate interests pursued by the controller or the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

The Hague Evidence Convention is not the exclusive process for conducting cross-border discovery in France.

Council Regulation (EC) No. 1206/2001 of May 28, 2001, on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (the "EC Regulation") entered into force in 2004. Largely inspired by the Hague Convention, the EC Regulation seeks to improve, by simplifying and accelerating, cooperation between courts of Member States of the European Union in the field of taking of evidence. The EC Regulation was necessary because the Hague Evidence Convention does not apply in some EU Member States.

Two major innovations should be pointed out:

Requests for taking of evidence are to be transmitted by the court before which the proceedings are commenced or contemplated (the "requesting court") directly to the competent court of another Member State (the "requested court") (Article 2).

Requests must be made using the prescribed form, to be completed in the official language (or one of the official languages) of the requested Member State or in another language acceptable thereto. Requests are executed by the requested court in accordance with the law of its Member State.

The execution of a request may be refused on a limited number of grounds.

A court of a Member State may, with the consent of, and under the conditions, if any, determined by, the central body or competent authority of another Member State, take evidence there directly, in accordance with the law of the Member State of the requesting court (Article 17).

These provisions contributing to rapid transmission and execution of requests between Member States' courts for the performance of taking of evidence attest to the European Union's desire to improve the efficiency of judicial procedures in civil or commercial matters.

Article 21 specifies that the EC Regulation prevails over provisions contained in bilateral or multilateral agreements or arrangements concluded by Member States, including the Hague Evidence Convention, in relations between Member States party thereto, but does not preclude Member States from maintaining or concluding agreements or arrangements between two or more of them, provided that they are compatible with the EC Regulation.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

France's "Blocking Statute" is the law of July 16, 1980, on the taking of evidence in view of judicial or administrative proceedings abroad, which amended the law of July 26, 1968.

Its main goal is to ensure that the taking of evidence in France for purposes of judicial or administrative proceedings commenced or contemplated in a foreign jurisdiction complies with French domestic rules or international agreements to which France is a party.

Article 1 of the Blocking Statute provides:

> Subject to international treaties or arrangements, it shall be prohibited for any individual who is a French citizen or has his usual residence in France and for any senior officer, representative, agent or employee of a legal entity having its registered office or a branch in France to disclose to foreign public authorities, whether in writing, orally or otherwise, in any place whatsoever, any economic, commercial, business, industrial, financial or technical documents or information, if such disclosure might impair French sovereignty, security, essential economic interests or public order.

Article 1A adds:

> Subject to international treaties or arrangements, it shall be prohibited for any individual to request, seek or disclose, whether in writing, orally or otherwise, any economic, commercial, business, industrial, financial or technical documents or information, if such actions aim at establishing evidence in view of foreign judicial or administrative proceedings, or in the framework of such proceedings.

Violation of the above provisions is punishable under Article 3 of the statute by six months' imprisonment and/or a fine of €18,000.

The proviso "subject to international treaties or arrangements" allows the general principal laid down by the Blocking Statute to be excluded by international provisions permitting and organizing the disclosure of documents or information to foreign authorities. This may be the case for bilateral conventions and for the Hague Convention of March 18, 1970, and Council Regulation (EC) No. 1206/2001 of May 28, 2001.

The enforcement of the French Blocking Statute provided an answer to the following question: Are the provisions of the Hague Evidence Convention mandatory or does the foreign authority have the possibility to choose the most appropriate method of taking evidence?

Contrary to U.S. courts, which place the Hague Evidence Convention on the same footing as other methods of discovery, French courts recognize its exclusive application pursuant to Article 1A of the Blocking Statute. As a matter of fact, French courts always invoke 1A of the Blocking Statute to deny disclosure requests made outside the judicial cooperation mechanisms established in the Hague Evidence Convention.

For example, by an order dated January 22, 1993, the urgent applications judge of the Regional Court of Nanterre denied a request by a foreign former head of state for certain French companies to be ordered to make disclosure of "full documentation," which could allow him to testify before a non-judicial body or bring suit in a foreign jurisdiction. The Nanterre judge held that the Blocking

Statute prohibited the disclosure of the information sought. He added that the judicial authority of the foreign country could have availed itself of the international-letter-of-request procedure under the Hague Evidence Convention.

Similarly, by a judgment dated July 20, 2005, the Paris Commercial Court denied a request for disclosure of bank records. The court held that the order of the New York District Judge directing the bank to disclose the records in question was contrary to the provisions of Article 1A of the Blocking Statute. Like the Nanterre judge, the Paris court noted that the foreign authority should have used the procedures available under the Hague Evidence Convention, the only legal instrument applicable between France and the United States in the field of taking of evidence.

In a recent decision dated March 28, 2007, the Paris Court of Appeal affirmed the interpretation of the Nanterre judge and Paris Commercial Court. The Paris Court of Appeal found that the French correspondent of an American attorney in charge of a lawsuit in the United States against French companies concerning the takeover of a U.S. insurance company had violated the Blocking Statute.

The correspondent had tried to obtain information, aimed at establishing evidence likely to be used in the U.S. lawsuit, from a former member of the board of directors of a French company. More specifically, he had requested information about the circumstances under which the board of directors resolved to take over the U.S. insurance company.

The appellate court found that the correspondent had violated Article 1A by acting outside the scope of the Blocking Statute, which allows evidence to be taken only as prescribed by applicable international conventions. The French correspondent, who was fined €10,000, was not a diplomatic officer, consular agent or authorized commissioner within the meaning of the Hague Evidence Convention. The French Supreme Court, in a decision dated December 12, 2007, upheld the position taken by the appellate court.

In penalizing evidence-gathering outside the scope of the procedures established in the Hague Evidence Convention, French judges mainly tend to stress the exclusive nature of the Hague exception to the prohibition laid down in Article 1A of the Blocking Statute.

c. *What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?*

In 1974, when the Hague Evidence Convention entered into force in France, France made a reservation under Article 23, declaring that it would not execute letters of request for pre-trial discovery.

In 1987, France made the reservation less stringent by allowing pre-trial discovery of particularized documents that relate directly and precisely to the subject matter of the dispute.

However, despite having relaxed its position with regard to other EU Member States, France still has the reputation of being hostile to U.S.-style discovery.

Germany

Axel Spies **- *Lead Editor***
Michael Molitoris, Dr. Thomas Roth, Andreas Tilp, Christian Schröder **- *Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Germany is a Civil Law country with a multi-tiered court system. The first two instances for civil matters are state courts: either local court (*Amtsgericht*) and regional court (*Landgericht*) or regional court (*Landgericht*) and higher regional court (*Oberlandesgericht*) – depending on the kind of an amount in dispute, the highest court of appeals is the Federal Court of Justice (*Bundesgerichtshof*). Although Germany has a federal structure with state courts, the rules on civil procedures are largely identical throughout the German Federal States, and that field of law is largely regulated by federal rules. The relevant (federal and state) law is codified, although case law plays an important role in interpreting the relevant provisions.

   The German Civil Procedures Act (*Zivilprozessordnung* – "*ZPO*") does not provide for pre-trial document discovery. Litigation is initiated when the plaintiff lodges his pleadings with the court. The judges are specially educated and trained; they are not elected but nominated by the Department of Justice of the respective Federal State. The jury system is not available in civil matters. A jury in the sense of a larger number of non-professional judges does not exist at all in German law. Claims and their defense must be described in sufficient detail and plaintiff and defendant must offer (but not submit) specific evidence in their briefs supporting their claims or counter-claims. German civil proceedings law follows the principle that the parties must submit all relevant facts and documents in support of their position, although there are some noteworthy exceptions, such as Sec. 142 ZPO (described below).

   Requesting and obtaining evidence takes place during a specific phase of a German trial. In most cases, supporting documents or other evidence must only be produced if the facts for which the documents serve as evidence are disputed between the parties. There are some noteworthy exceptions, for instance, in litigations enforcing checks or bills of exchange. It is usually not necessary to attach a document to a pleading – it suffices that the party describes how it will produce evidence in case that the opposing party disputes a fact (*e.g.,* "testimony of witness XYZ for the fact that the defendant was present during the meeting"). In practice, however, the plaintiff or defendant often attach copies of key documents or excerpts to their briefs to illustrate their case and claims.

   The ZPO distinguishes between five categories of evidence: inspection, witnesses testimony, expert's opinion, documents and interrogation of a party. The term "documents" is defined broadly (as a "written expression of any thought") so that it covers letters, written notes, emails and the like.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion*

of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.

There is no automatic obligation to disclose or produce documents absent a court order. There is no "discovery phase" as such in German civil proceedings. The principle is that each party needs to produce the evidence necessary to support its own arguments. Taking evidence requires an "evidence" motion to the court by a party describing: (a) the fact in issue, and (b) the means of evidence (how the party intends to obtain the evidence).

Based on this motion, and potentially a court hearing, the judge then decides whether:

- the facts in issue are relevant to the outcome of the case, and
- the facts are disputed so that taking the evidence is required to clarify the facts.

There are some exceptions to the rule that a party that has the burden of proof in a proceeding is obligated to produce the relevant evidence. First, German law and/or relevant case law provides *prima facie* rules (*Anscheinsbeweis*), or shifts in the burden of proof to the defending party. For instance, in an insolvency case, it may be upon the defendant to present documents that demonstrate that he has not delayed the filing of a bankruptcy petition on behalf of his company.

Moreover, a key provision for a pending civil proceeding is the (recently revised) Sec. 142 ZPO that gives the judge significant discretion to order that documents be produced:

> (1) The court may order that a litigation party or a third person must produce certificates and other documents that he has under control and that are referred to by a party. For this purpose, the court may set a deadline and may also order that the documents shall remain with the clerk of the court of for a specific time period.
>
> (2) Third persons are not obliged to present documents if their production is too burdensome or infringes with their right to refuse to give evidence under Secs. 383 to 385.…
>
> (3) The court may order that in case that the documents are in a foreign language that translations must be presented that must comply with the rules and guidelines of the State Administration of Justice. Such a translation shall be deemed correct if so certified by the translator. The certification shall be placed on the translation and must indicate the location and the date of the translation, information on the translator and must be signed. Evidence that the translation is incorrect or incomplete is admissible. The first sentence of this sub-paragraph shall not apply to third persons.

(a) According to subsection 1 of this provision, a court is entitled to order – even without a motion by a party – that the parties in a civil proceeding (and third parties) must produce written documents they have under their (factual) control. Such order, which is in the discretion of the judge, may be rendered in any phase of the trial, but not before the litigation is launched. The term "documents" in this provision is defined broadly and covers agreements, correspondence, patient documents (*e.g.,* prints of X-rays), drawings, plans, and – as described above – all documents that are stored electronically. There is no specific "purpose" of the production required as long as the documents serve to shed light on the facts in a proceeding by providing more details to the pleadings of a party.

A judge could even issue an order pursuant to Sec. 142 ZPO if he believes that the documents are necessary to give him a better picture of what this case is about, provided that the documents are substantial for the outcome of the litigation. The more important the document is for the outcome of the litigation, the narrower the room for discretion the judge has to deny a motion for production of evidence. This power of the court to order the production of documents must, however, not infringe on the general principle of German civil procedure that the parties and not the court must produce the evidence. Therefore, the judge must limit its orders to the minimum amount of documents that is necessary for his/her understanding of the case and that is indicated by either party. The judge must also strictly refrain from any order that may interfere with his/her neutrality. In any event, the decision can be appealed by either party (dissenting OLG [Higher Regional Court] Karlsruhe, OLG-Report 2005, p. 484).

A pre-condition for an order according to Sec. 142 ZPO is the plaintiff, defendant or a third party exerts factual control (possession) over this document. The document must already exist (for instance, plans of a building that still must be drawn by a party would not be covered by this Section). Moreover, a party (plaintiff or defendant) must refer to the document in one of his pleadings. There is some debate among scholars on how specific this reference must be; German courts only impose a low threshold by stating that it is sufficient if the reference to the document in a pleading is specific enough so that the party possessing the document can identify it. A mere statement in a pleading that a document "usually exists" in the business of the other party and therefore should be produced is not sufficient. Sec. 142 ZPO does not allow fishing expeditions ("*Ausforschungsbeweis*").

"Data protection" is not explicitly mentioned as a reason for the judge to deny an order pursuant to Sec. 142 ZPO; however, there are some court decisions that if there is a "justified interest" of a party to keep the document secret, an order to produce the document should not be issued. If highly confidential business secrets are required to be produced, the judge may grant protection to the requested party by allowing only the adverse attorney and not the adverse party to review the processed documents. An order can also be denied if producing the document would infringe on the attorney-client relationship of the party. However, the mere fact that producing the document would incur the risk that a party be prosecuted under criminal law is not sufficient to deny an order.

(b) Sec. 142 para. 2 ZPO contains a restriction on issuing an order that would direct a third party to produce a document if the third party has a right to deny testimony according to the general provisions of the ZPO (the most important one being the protection self-incrimination), or if it is otherwise not unreasonable ("*nicht zumutbar*") for the third party to produce the document. The German literature has criticized the latter provision as being overly vague – for instance, a party could claim in rare instances that it poses an undue burden to find the document or that it needs the document for its daily business. In any event, the third party must bear the costs for producing the document. As part of the initial pleadings in litigation, a plaintiff or a defendant can move the court to issue an order pursuant to Sec. 142 ZPO so that a document be produced.

(c) Sec. 142 para. 3 ZPO gives that judge additional authority to oblige a party of a litigation that must produce a document that is not in German to submit a translation. However, this is not a mandatory requirement: if the judge deems that he and the parties are sufficiently fluent in the foreign language, as it happens frequently with documents in English, he may order that only the document in a foreign language be produced and waive the translation requirement. Usually, German courts have local rules on who is entitled to translate a document that is introduced in a civil proceeding (rules court-admitted translators). The winning party may move the court to receive reimbursement for the translation costs by the other party.

In the court order pursuant to Sec. 142 ZPO, the judge may set a reasonable deadline by which the document must be produced and submitted to the Clerk of the Court. A party missing the deadline could face court sanctions.

In addition to Sec. 142 ZPO and production requirements in child support and alimony matters, there are a number of specific provisions outside of the ZPO and the Criminal Procedures Code (*Strafprozessordnung*, "StPO") that require a party to produce documents, such as:

- Sec. 90 para 2 General Tax Code contains broadly defined requirements to produce documents that are relevant in a tax proceeding to the German IRS, irrespective of whether the documents are located in Germany or abroad.

- Sec. 258 Code of Commerce (HGB) states that in a business-to-business litigation the court (with or without being based on a motion of a party) may oblige a party to present its "business books." This term is defined broadly and covers balance sheets, audit certificates and the like. These are not necessarily books in the actual sense of the word and can be stored electronically (Sec. 239 para. 4) if this storage is in compliance with the bookkeeping rules and the data can be converted into "readable form" within an appropriate time period. In addition, Sec. 261 Commercial Code states that if there is a dispute between businesses, and a party is obliged to make available such information stored on picture media or as data in electronic data bases, the other party can demand hard copies. The producing party must bear the costs for providing hard copies to the other side or presenting the document in a form that allows that the document be read without further technical means.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Germany, a civil law country, does not know "pretrial discovery" from a third party. It would also be difficult to enforce requests from U.S. courts that allow such discovery in Germany because Germany has issued a reservation according to Art. 23 Hague Convention on Evidence that the country will not process requests from the United States for "pre-trial discovery." The reservation does not make a distinction between parties and non-parties. This means that the Central Authorities in Germany will not process letters of requests from the United States courts aiming at "pre-trial discovery." In some cases, the German Central Authorities may pass letters of requests on to the German local courts if the U.S. court requests specific documents from the party or non-party in Germany, the documents are necessary for rendering a decision and the U.S. court proceeding is already pending. In other cases, the plaintiffs sue the other party directly in the German courts and try to convince the judge to grant discovery of specific documents and move the court to grant an order under Sec. 142 ZPO, which is applicable also to non-parties, as mentioned above.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

There are no document preservation rules in Germany as under the U.S. Federal Rules of Civil Procedures. While the parties have no general legal obligation to preserve documents with regard to a proceeding, a party shown to have destroyed a document runs the risk that the competent court will draw negative conclusions from such behavior under Sec. 286 ZPO. However, apart from the Civil Procedure Rules, specific laws, *e.g.,* tax laws or the Commercial Code may require companies to preserve certain documents. For example, Sec. 257 HGB contains specific requirements on business-related documents that a business must preserve for a period of 6 years – in certain cases 10 years. The provision only covers the documents that are enumerated under this provision, such as balance sheets, business correspondence, etc.

The ZPO provides for a separate judicial procedure to preserve evidence (Sec. 485 – *Beweissicherungsverfahren*) that can be launched even before the actual trial commences. If there is a concern that evidence will disappear or be tampered with, otherwise be lost or taking evidence at a later state would impose an undue burden on the party a motion to preserve evidence can be filed at any time – also before a formal complaint is filed. In order to launch this procedure to preserve evidence, there must be a motion and the court must consent. This procedure only covers certain means of evidence, namely evidence by actual inspection, hearing witnesses, or experts, not by way of the production of documents. While a document production cannot be achieved in this proceeding, it may provide the plaintiff with an indirect means to achieve a "freeze" to avoid that electronic documents are destroyed or manipulated.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

   If a party does not comply with an order to produce certain documents (Sec. 142 ZPO), such order will not be enforced or punished with, *e.g.,* criminal sanctions. The non-production will, however, be taken into consideration by the judge when assessing the claim. *See* Sec. 286 ZPO. The judge may, therefore, draw negative conclusions.

   There are specific stipulations in the German Criminal Code sanctioning the deliberate destruction or suppression of documents. There is no general rule on the preservation of documents in the ZPO: The civil judge has discretion under Sec. 286 ZPO on how he evaluates the fact that a document has disappeared or is otherwise no longer available, for instance by ruling that there is a shift of the burden of proof because of this.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

   The principle is that the party that loses the litigation must bear the "necessary costs" of the opponent to the extent that they are "connected with the litigation" (Sec. 91 ZPO). In a proceeding to maintain or "freeze" evidence (Sec. 485 ZPO) outside of the main proceeding, the judge may rule on the costs separately.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

   The general rule is that "electronic" documents are treated as every other document. In practice, a party building its argument on an electronic document must authenticate the email by demonstrating when the email, file, etc. was created and where it was stored and must establish a chain of custody. The concrete standards depend on the circumstances of each case, for instance, the judge would consider the procedural context (other evidence pointing into the same direction, for instance). The problem that parties are facing frequently is how to demonstrate that the document actually stems from the issuer. While German judges have significant discretion on how they classify electronic evidence (*e.g.,* emails or electronic files), many of them do not accept printed emails or simple hardcopies of an electronic file as a "document" – mainly due to manipulation concerns. In this case, an email could be still introduced into the trial by way of "evidence by inspection." This means that the party would be allowed to present the hardcopy to the judge to identify that such a document exists, but it would not be accepted as a piece evidence to prove that its content is true (if, however, a witness is confronted with this document, his statement could be used as evidence).

   It is upon the judge, potentially on the basis of expert testimony, to decide whether the document is authentic or not (Sec. 416 ZPO).

There are a few exemptions to this authentication requirement, if the electronic document bears a (registered) electronic signature of the issuer in compliance with the Act on Electronic Signatures. In this case Sec. 371a para. 1 ZPO stipulates that it is presumed that the electronic documents stems from the person whom the (registered) signature key belongs to – rebuttal evidence against this presumption is possible.

There are also new provisions in the ZPO on the legal requirements that an electronic document issued by a *public* authority must fulfill to be admitted as evidence (Secs. 371a, 416a ZPO): In order to be introduced into the trial as a "document," such letter/email etc., must bear an "authentication mark" (*e.g.,* an official stamp and signature) by the authority or a specific electronic signature as foreseen by the Act on Electronic Signatures.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   There are no such rules in the ZPO – other than the mentioned Secs. 371a, 416a ZPO.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

   There are no such rules in the ZPO.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

    There are no such rules in the ZPO. As for the general rules, *see* the response to question 4 above.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

    There are no such rules in the ZPO.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

    There are no such rules in the ZPO.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

    There are no such rules in the ZPO.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

    There are no such rules in the ZPO. However, courts will probably take into consideration any non-diligent production/preservation of documents (after an order to produce certain documents) when assessing the overall evidence in accordance with Sec. 286 ZPO and may draw negative conclusions from such behavior. Regarding the authentication of the evidence, please note the response to question 7 above.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

    According to the ZPO, documents that were "brought into circulation" without the consent of the issuer, can be rejected by the judge as evidence. Pursuant to Sec. 383 (1) (6) ZPO attorneys and in-house counsel acting in their capacity as legal advisors are entitled to refuse to give evidence on any information provided to them while

performing such services. However, this does not apply to information obtained while performing management or similar duties or obtained before they were instructed as legal advisor. This right is also extended to personnel assisting the in-house counsel in the performance of legal work. A counsel has the right to refuse to produce documents to the same extent as he is entitled to refuse testimony (Sec. 142 (2) ZPO), which means that the judge must not base his decision on documents that are "privileged" under these provisions (Sec. 383 (3) ZPO). If an attorney violates his obligation to keep his communication with the client secret, he may face sanctions under the Federal Bar Rules (BRAO) or under Sec. 203 Criminal Code (breach of professional secrecy). Moreover, there are some other professions (*e.g.,* medical doctors etc.) subject to professional secrecy.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

The principle is that the party that loses the litigation must bear the "necessary costs" of the opponent to the extent that they are "connected with the litigation" (Sec. 91 ZPO). In a proceeding to maintain or "freeze" evidence (Sec. 485 ZPO) outside of the main proceeding, the judge may rule on the costs separately.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

No, but see above response to question 4 on the judicial procedure to preserve evidence (Sec. 485 ZPO). In addition, there are additional data retention requirements in others laws. For instance, the EU's 2006 Data Retention Directive and new national law mandates the retention of all traffic data (call data, e-mail address fields, etc.) by telecommunications carriers and Internet Service Providers from 6 months up to two years for law enforcement purposes. This law has been challenged before the German Federal Constitutional Court.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

A number of large U.S. service providers that manage litigation documents are active in Germany. Various companies in Germany are already specializing in offering electronic discovery services, such as collecting, filtering and securing electronic files and records, examining hardware, etc.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

See responses to questions 20 and 21 below.

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

    a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

    b. *The legal definition of "personal data" and "processing" of data within your jurisdiction.*

    c. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    d. *Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.*

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

The German ZPO does not contain rules on data protection and decisions of higher civil courts on this issue are relatively rare. The German Judicial Constitutional Act (*Gerichtsverfassungsgesetz)* provides for very general rules to protect business secrets of a party, *e.g.,* by excluding the public form a hearing (Sec. 171b). Sec. 299 (2) ZPO allows a presiding judge to impose restrictions on the inspection of documents by the public. German data protection authorities have not (yet) explicitly addressed the issue of e-discovery – rather, the current discussions take place on the EU level between the members of the Article 29 Working Party where German data protection agencies directly and indirectly play an active role.

The German (Federal) Data Protection Act (*Bundesdatenschutzgesetz* or "BDSG") does not specifically address if and how personal data can be introduced into a civil or criminal litigation. The BDSG, in spite of various sector-specific regulations, remains the omnibus law for data protection in the public and private sector. Therefore, it would also apply in civil and criminal proceedings, although a civil judge will first examine the rules in the ZPO regarding the production and protection of evidence before recurring to the BDSG. Another difference is that the BDSG only protects individuals ("data subjects") and their personal data (however, their name could appear in a company's name and would be protected), whereas the ZPO governs any form of evidence. Data processing is defined widely as the collection, storage, modification, transfer and deletion of personal data (Sec. 3(4) BDSG).

The BDSG contains provisions that personal data can only be collected or allowed by a law/ statute or the individual has given his/her prior consent (Sec. 9 (1)). In general, a private entity is not allowed to make use or transfer personal data for other purpose than for which the data have been collected (Sec. 28 (1)). Moreover, the BDSG provides for specific rules covering so-called "sensitive data" that are protected by special rules (the German law refers to this category as "special classes of person-related data" that contain the following information):

- race/ethnic origin,
- political opinion,
- religious and political affiliation,
- affiliation with a trade union,
- health data,
- sexual orientation.

The distinction between sensitive and non-sensitive personal data is based on EU law. The idea is that sensitive data should not be processed without explicit consent of the individual. The distinction and filtering of electronic documents with sensitive data becomes complicated and questionable when sensitive information is implicitly contained in "normal" personal data (for example, buying cigarettes = being a smoker = having a higher risk of cancer).

The BDSG also stipulates that personal data may only be processed for the purpose for which it has been collected – which is another key principle of German data protection law. Companies must not collect and store personal data arbitrarily for later use. This may, for instance, cause problems for US requests for "litigation hold" of data stored in Germany that were not collected for this purpose. Moreover, the individual must be told at the time of collection the purposes for which needed. If the purpose of the data collection changes at a later stage, the data subject must consent before his/her data can be used for the new purpose, unless the BDSG provides otherwise, for instance, if the company does not know and cannot find out with reasonable means where the individual is. This principle could stand against collecting personal data in one litigation proceeding and then using the data in another proceeding, unless there are overriding interests, such as criminal intent of the individual, etc.

Given that in a civil case the judge plays a key role by issuing "evidence orders," as described above, the party collecting the evidence could move the court to approve the data collection and eventually the data transfer. Although such a motion is possible in theory, this strategy is rarely pursued and has not been tested in the higher courts. What happens more frequently is that a party makes an upfront attempt to limit the scope of the collection in a defensible matter and tries to negotiate the matter with counsel of the opposing party. In Germany, judges usually are only presented with the results of the e-discovery, once the judge has issued an "evidence order" (see above), and don't rule on the issue whether the evidence was obtained legally, unless the other party objects and files a motion to this end.

Specific issues arise if employee data is collected for e-discovery purposes: there is some case law in Germany (and some guidance from the federal and state data protection agencies) on the treatment of employment data (name, address, etc.) and the personal data that employees create or otherwise process (*e.g.,* emails and other electronic documents). The data protection rules in Germany state that all personal data (emails, electronic lists of names, etc.) are protected, however, certain data that fall in the scope of a job performance or other business-related activity of an employee ("*Geschäftsdaten*") belongs to the employer. Some companies in the communications sector (carriers, ISPs) are required by law to store certain categories of (employment) data for law enforcement purposes (telephone records, email headers).

The upshot on the German rules on employment data is that there is an area of "private" communication (private emails, private telephone calls, etc.) that is protected by the law, in particular by Sec. 88 Telecommunications Act (Guarantee of "Telecommunications Secrecy"), if the employee uses the telephone or his computer at work for private communication (it is disputed where private communication on mere Inter-Corporate Network would be protected.). This "private communication" would probably not be discoverable, unless the individual or the works council of the company consents.

The distinction between what is "private" communication and other employment-related communications that could be collected as evidence is not easy. Some companies forbid their employees completely to use their computer /telephone for private communication, others provide different log-ins or mailboxes (one for employment-related, one for private communication). However, if the employer has allowed the private use of the Internet, he must respect the right to communications secrecy of the employees, pursuant to which data may only be processed or used, to the extent that the information is necessary for the provisioning of Internet services or billing. Since the employer has a justified interest in preventing abuse or criminal activities not only regarding work-related Internet access, but also regarding any private use of the Internet, he is

entitled to allow the private use of the Internet only under certain conditions regarding the time periods, the admitted areas and regular checks. For a third party, this could mean that such "private" communication is not discoverable and must be filtered.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

There are two potentially relevant bodies that should be involved in the electronic data collection process: the In-house Data Protection Officer and the Works Council of the company where the data is located. There is no notification requirement to the data protection agency before the discovery can commence. There is no information that German data protection agencies have actually interfered and blocked data transfers from Germany to the United States for discovery purposes.

The concept of having an in-house data protection officer ("*Betrieblicher Datenschutzbeauftragter*" – "DPO") is probably the lynchpin of the data protection concept for private and public entities in Germany. The BDSG stipulates that larger companies processing personal data in Germany must appoint a DPO, in particular if the company has more than 20 employees that process personal data. In any case, a company can also appoint a DPO on a voluntary basis at any time. A DPO is an employee of the company that appoints him. He is not imposed on the company or otherwise assigned by the DPA.

A DPO's primary tasks are to advise the management of the company on privacy matters, to control the processing of personal data within the company and to be the interface with the data protection authorities. Under the BDSG, companies are free to choose an internal or external DPO. DPOs are usually very familiar with the problems of the entity on site where they work. Although there is no direct obligation in the BDSG, actively informing and involving the data protection officer within the company is a standard procedure in many discovery cases. This will allow the data protection officer to consult with the state data protection agency in advance to ensure that there are no objections. Informing the management of the company of the discovery and the data transfer is another avenue, unless, of course, the investigation is directed against a member of the management who potentially will alter, block or destroy electronic evidence.

Moreover, most larger German companies have a works council that is the representative body of the employees which has to be established if they vote to have one. In particular, the works council must consent to measures pertaining to all questions of employees' surveillance and control like, for example, introducing telephone monitoring. If consent is withheld by the works council for no valid reason, its decision can be overruled by the labor court having jurisdiction in this matter. In some instances, prior consent of the works council may be sufficient to allow a client implement to a policy for the transfer of work-related data and electronic documents to be used in a legal proceeding (instead of obtaining consent from each individual employee). In others, prior approval

of a company policy addressing investigations by the works council may be required (*e.g.,* formal consent in a company's whistleblower scheme under the Sarbanes Oxley Act).

Given that the German law distinguishes between information that belongs to the company and "private" information that belongs to the employee (*e.g.,* private emails) filtering out the relevant information on site may be required to ensure that taking evidence does not infringe on data protection law. This filtering requirement could mean that the client opts to outsource the filtering of the information in the computer systems at the plant/office in Germany, *e.g.,* to a local attorney and/or a certified litigation service provider. This person or organization then selects the information that is relevant to the cases (*e.g.,* all emails that only refer to a certain event that are not deemed "private communications" under the applicable rules and guidelines). Involving a local attorney on site during this process could ensure that no client-attorney related documents or private correspondence of employees are collected. Only the screened and filtered information is then provided to the client.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The Hague Convention is not the exclusive process for sending personal data from Germany to the United States. The relevant provisions in the BDSG governing international data transfers out of Germany *do not* stipulate that a German judge or a German data protection agency must consent to the individual data transfer out of the country. Rather, the BDSG allows the data transfer if the recipient of the data complies with certain legal standards and safeguards. It is on the sender and on the recipient (joint and several liability) to ensure compliance and they bear the legal risk that the data transfer is deemed illegal.

From the German perspective, the German BDSG remains applicable if personal data from Germany is sent to the United States. However, the EU's 1995 Data Protection Directive and provisions in the BDSG (in particular its Sec. 4b) prohibit the transfer of personal data to non-EU nations (for *any* purpose) that do not meet the European "adequacy" standard for privacy protection. The EU has identified the United States as a country that fails to offer "adequate" privacy protection. Realizing that it would be impossible to prohibit any and all transfers of personal data to the United States, the EU and U.S. have tried to bridge the gap and developed a "Safe Harbor" concept for international data transfers. This concept consists of a set of rules (the "Principles" and the answers to Frequently Asked Questions "FAQs").

In addition, so-called contractual Standard Clauses for personal data transfers to the United States may be used by the data transferring parties. Some U.S. companies with branches in Germany have voluntarily agreed to implement the Safe Harbor principles in order to be deemed in compliance with EU privacy protection regulations, but there is no provision under the EU Directive or German

law that would generally exempt e-discoveries from the general prohibition to transfer personal data from Germany in the United States.

However, even in case of a lack of sufficient data protection in the receiver's country, Sec. Sec. 4c (1) (4) BDSG may apply. This provision allows the transfer of personal data out of Germany, even to a country "non-adequate" data protection if the "transfer is necessary to raise a claim or for exertion of a right or a defense against a claim "at the court." Scholars and the Federal Data Protection Commissioner, however, require a binding court order to produce such information and the scope must be limited to the extent absolutely necessary for the compliance with such court order. In addition, parties may have to search for Protective Orders in order to limit the disclosure of the submitted information only to the necessary recipients. There is also no blocking statute in Germany that generally forbids the transfer of personal data to the United States for discovery purposes.

If a U.S. court asks a German court to collect the evidence, legal assistance is provided through the Hague Convention; however, the rules of the BDSG for data transfers to other countries apply irrespective of whether documents are produced on the basis of a letter of request, or on a voluntary basis. So far, no case has been reported that the Central Authorities in Germany have refused to process a letter of request from the United States due to privacy concerns under the BDSG.

As described in the response to question 21, in many cases not all personal data cannot be legally exported or must be filtered before it can be used. This requirement would apply irrespective of whether the litigation takes place in Germany or elsewhere. In some cases, parties in Germany have argued that the transfer of personal data that is potentially relevant in a civil proceeding to a law firm in the United States is covered by the attorney-client privilege and Sec. 4c (1) (4) BDSG. The latter provision allows the transfer of personal data out of Germany, even to a country "non-adequate" data protection if the "transfer is necessary to raise a claim or for exertion of a right or a defense against a claim "at the court."

This argument has not been tested in German courts. While there is significant trust of a German court that lawyers in the United States will keep the personal data they receive in connection with a court proceeding safe, it is not clear how far the scope of this Sec. 4c (1) (4) BDSG goes: in particular, it is not clear whether the receiving U.S. attorneys must keep the data separate, and in which instances the attorneys are allowed to make the data available to the court or the opposing party or experts in the United States. Some scholars suggest that such data from Europe can only be introduced in a proceeding under a Protective Order by the U.S. court. If a third party provider is used to collect and transfer the data for a litigation in the United States, such provider could register under the above-mentioned EU/U.S. Safe Harbor Principles for international data transfers that are administered by the U.S. Department of Commerce or use the standard contractual clauses for international data transfers that the European Commission has developed.

The issue of transferring discovery data to the United States is in a state of flux and German data protection agencies will likely follow the recommendations (opinions) of the Article 29 Working Party, the body of data protection experts advising the European Commission on the issue of international data transfers for discovery purposes. The Article 29 Working Party has the issue on their agenda list for this year.

Ireland

Aoife Gaughan - ***Lead Editor***
Lisa Broderick, Sharon Daly - ***Contributing Editors***
Stewart Room, Conor Crowley - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Ireland is a Common Law jurisdiction with a written Constitution and is a member of the European Union.[148] There are four civil court jurisdictions: the District Court and the Circuit Court, which both have limited jurisdictions and are organised on a regional basis,[149] the High Court, which has full original jurisdiction and the Supreme Court, which is the Court of final appeal. There is also a specialist Commercial Court, which is a division of the High Court that was established in order to provide efficient and effective dispute resolution in commercial matters. The Commercial Court began hearing cases on 12 January 2004 and makes effective use of case management procedures, imposing deadlines in order to move commercial disputes to speedy resolution: either to settlement (including via mediation) or to trial. Most cases are dealt with in less than 6 months and there can therefore be tight deadlines for discovery. The Commercial Court deals with commercial proceedings in relation to certain defined categories[150] where the value of the claim/counterclaim is not less than €1,000,000. It also hears all intellectual property claims, judicial review of appropriate regulatory decisions and other matters that it deems are appropriate to be heard by the Commercial Court. Its rules specifically provide for the electronic filing of documents although this has not yet fully been implemented.

   Pre-trial discovery of documents is permitted in Ireland. There is no oral discovery or deposition procedure, other than in exceptional circumstances, where evidence can be taken on commission (for example, where a witness is likely to be too ill to give evidence at the hearing).

   Documentary discovery in Ireland is a two-stage procedure involving the disclosure on affidavit listing the relevant documents, followed by the inspection of such documents. However, a party may claim legal professional privilege in relation to certain documents. The practice is to list these documents as privileged and not to produce them and then the party seeking discovery can seek to challenge the claim of privilege, which would ultimately be decided by the court.

   Discovery is a discretionary process that is governed by the procedural rules of court. The Rules of the Superior Courts apply in the High Court and the Supreme Court.[151] These rules are interpreted by the courts in matters which come before them, which develop the case law. Whereas in the past, discovery of documents in Ireland was quite broad, allowing almost blanket discovery, the scope of discovery was considerably narrowed by amendments to the Rules of the Superior Court in 1999,[152] which shifted the burden of proving that discovery was necessary onto the party seeking discovery. These rules came into operation on 3 August 1999 and require the party seeking discovery to specify the precise categories of documents sought. The rules require that an attempt first be made by parties to agree terms for voluntary discovery. In the event that voluntary discovery is not possible, the party seeking discovery must verify on affidavit (a sworn written statement of fact) (1) that the categories of documents sought are necessary to fairly dispose of the matter, or are necessary for saving costs and (2) they must furnish the reasons why *each* category of documents is required to be discovered. The amended rules therefore seek to avoid excessive, over burdensome discovery or a potential "fishing expedition."

[148] Article 34.1 of the Irish Constitution provides that "Justice shall be administered in Courts established by law by judges appointed in the manner provided by this constitution, and, save in such special and limited cases as may be prescribed by law, shall be administered in public."
[149] The District court has a limited civil jurisdiction of claims up to €6,350 and the circuit court can hear civil claims up to a maximum of €38,092.
[150] *See* Rules of the Superior Courts (Commercial Proceedings) 2004 (SI No. 2 of 2004).
[151] There are separate procedural rules for the circuit and district courts, which are not covered by this document.
[152] Rules of the Superior Courts (No. 2) (Discovery) 1999 (SI No. 233 of 1999).

Freedom of Information requests may also be made in relation to prescribed public bodies in accordance with the Freedom of Information Acts 1997 and 2003.[153] This is entirely separate to the discovery process and, for example, it is possible to make a Freedom of Information request prior to instigating proceedings against public bodies. The prescribed public bodies include government departments, state agencies, county and city councils, regional authorities, the health service executive, voluntary hospitals, third level institutions and the fisheries boards.

Data Access Requests are also becoming a common tool in disputes. These are provided for in s4 of the Data Protection Acts and give individuals the right of access to personal data held by data controllers. Once an appropriate request is made in accordance with the legislation, individuals must be informed of any data personal to them in the data controller's possession. The fact that an individual is involved in litigation does not preclude them from making a data access request or contemplating same.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

Scope

Order 31 rule 12 of the Rules of the Superior Courts governs inter party discovery. The scope of discovery in each case is determined either by agreement between the parties where voluntary discovery is obtained, or by order of the court. Discovery must be requested by one of the parties and cannot be ordered *ex officio* by a judge. All documents under each of the agreed or ordered precise categories of documents relating to the matter in question which are or have been in the possession or power of the party against whom discovery is sought must be disclosed on affidavit to the other party. Privileged documents are discoverable but do not need to be produced. They do however need to be listed in a separate schedule in the affidavit. This obligation applies even to documents that may damage the party's case, help their opponent's case or lead to a train of inquiry. Not all litigants appreciate this, which can lead to the provision of inadequate discovery. The Litigation Committee of the Law Society in Ireland[154] has recommended that Order 31 rule 12 be amended so as to provide that the extent of a party's obligations should be spelled out in plain language in their affidavit. It is hoped this would reinforce their understanding of what is required.

Documents containing business secrets are discoverable, but the court may impose restrictions on those to whom access is provided (*e.g.,* just to an expert or legal team). It is generally accepted that documents that are provided on foot of an order for discovery are subject to an implied undertaking that they can only be used for the purpose of that action and that to go beyond that would be contempt of court. Indeed, the Chief Justice of the Supreme Court (Finlay, CJ) stated in *Ambiorix Ltd. v. Minister for the Environment* (No. 1)[155] that:

> . . . [a] party obtaining the production of documents by discovery in an action is prohibited by law from making any use of any description of such documents or the information contained in them otherwise than for the purpose of the action. To go outside that prohibition is to commit contempt of court.

However, this is not an absolute prohibition. If special circumstances exist and it can be shown that no injustice would be caused to the person giving discovery, the court may allow such documents to be used.[156]

Voluntary Discovery

Voluntary discovery must first be sought pursuant to Order 31 rule 12 Sub-Rule 4, noting that failure to make discovery may result in an application pursuant to Order 31 rule 21.[157] A request for voluntary discovery must be by letter in writing and must specify the precise categories of documents in respect of which discovery is

[153] *See* the website for the Office of the Information Commissioner for more information in this regard: http://wwwcic.nov.ie/en/ which also provides a full list of the prescribed bodies.
[154] Discovery in the Electronic Age: Proposals for Change.
[155] *Ambiorix Ltd. v. Minister for the Environment* (No. 1) [1992] 1 I.R. 277, at p. 286.
[156] *Roussel v. Farchepro Ltd* [1999] 3 I.R. 567.
[157] Order 31 Rule 21 of the Rules of the Superior Courts ("RSC"). If any party fails to comply with any order to answer interrogatories, or for discovery or inspection of documents, he shall be liable to attachment. He shall also, if a plaintiff be liable to have his action dismissed for want of prosecution, and, if a defendant, to have his defence, if any, struck out, and to be placed in the same position as if he had not defended, and the party interrogating may apply to the Court for an order to that effect, and an order may be made accordingly.

sought and furnish the reasons why each category of documents is required to be discovered. The party seeking voluntary discovery must then allow a reasonable period of time for such discovery. Where voluntary discovery is agreed pursuant to Order 31 rule 12 sub-rule 4, it has the effect as if it were directed by order of the court.[158] In cases where a request for voluntary discovery fails, is refused, ignored or neglected by the other party, the party seeking discovery may apply for an order for discovery from the court.[159]

If an applicant fails to seek voluntary discovery, the court may refuse their application for discovery by reason of non-compliance with sub-rule 4. However, a court may permit an application without the necessity for prior written request for voluntary discovery if the court decides it is appropriate due to the urgency of the matter, consent of the parties, other circumstances or the nature of the case. The courts are likely however to allocate costs to any party that fails to adhere strictly to the letter of the rules.

Specify Precise Categories of Documents

Prior to 1999, discovery was fairly straightforward. However, as it effectively allowed blanket discovery without the need to specify and justify detailed categories, the costs of discovery were often very significant and this old system regularly produced large numbers of documents that had no real relevance to the issue between the parties.[160]

Amendments to Order 31 rule 12[161] came into operation on 3 August 1999 effectively to attempt to limit such "fishing expeditions." Subsection one of which provides:

> (1) Any party may apply to the Court by way of notice of motion for an order directing any other party to any cause or matter to make discovery on oath of the documents which are or have been in his or her possession or power, relating to any matter in question therein. Every such notice of motion shall specify the precise categories of documents in respect of which discovery is sought and shall be grounded upon the affidavit of the party seeking such an order of discovery which shall:
>
> (a) verify that the discovery of documents sought is necessary for disposing fairly of the cause or matter or for saving costs;
>
> (b) furnish the reasons why each category of documents is required to be discovered.

The courts have made clear that the reasons given must refer specifically to the pleadings if they are to be deemed central to the issues.[162]

Discretionary Process

Discovery is a discretionary process and not a right. On hearing an application for discovery, the court may decide to make the order, limit it to certain classes of or to specific documents or grant it on terms as to security for the costs of discovery. Alternatively, the court may refuse or adjourn the application if it decides such discovery is not necessary, or that it is not necessary at that stage, or if the party applying for discovery has not complied with the rules[163] as to voluntary discovery. The court may also choose to reject an application if the information could be obtained in some other way, for example, by the service of a notice to admit facts or documents. Fennelly, J. indicated in *Ryanair v. Aer Rianta Cpt.*[164] that the behaviour of the opposing party is also

[158] RSC Order 31 Rule 12 Sub-Rule 4(2).

[159] In 2001, the then President of the High Court, Mr Justice Morris, held in *Swords v. Western Protein Ltd.* that where the letter used to seek voluntary discovery failed "to pinpoint the documents, required and, give reasons why they were required," the Master of the High Court does not have the power to determine the application. Following on from that decision, the Master of the High Court (who deals with the majority of applications for discovery) struck out a variety of applications on the basis that the voluntary discovery requests failed to sufficiently identify the documents sought and the reasons for which their discovery was required.

[160] In 1999, in *Brooks Thomas Ltd. v. Impac Ltd*. the plaintiff sought discovery of all documents "indicating the [defendant's] approach to management consultancy", however, the Supreme Court was of the view that these documents were not necessary in order to succeed in the case. The Supreme Court went on to recommend that the Superior Court Rules Committee should consider amending the rules governing discovery to curb general discovery, which led to the 1999 amendments. In *KA v. The Minister for Justice, Equality and Law Reform,* Ms. Justice Finlay Geoghegan stated in relation to the limitation on discovery, inter alia, that ". . . it is that it must not be considered to be a fishing exercise …, it is not sufficient for an applicant simply to make an assertion not based on any substantial fact and then seek discovery in the hope that there will exist documents which support the contention."

[161] As substituted by Statutory Instrument 233 of 1999.

[162] *Medtronic Inc., and Ors v. Guidant Corp. and Ors* [2007] I.E.H.C. 37.

[163] Sub-rule 4(1).

[164] *Ryanair v. Aer Rianta Cpt.* [2003] 4 I.R. 264.

relevant. A variety of factors are clearly capable of influencing the court. However, the court is also willing to take positive steps to amend categories to facilitate discovery where it is satisfied that it is necessary.

The Irish courts will not make an order for discovery if it is not necessary either for (a) disposing fairly of the cause or matter or (b) for saving costs. It is therefore necessary for the party seeking discovery to satisfy this criterion on affidavit.[165]

While the current discovery rules require parties and the courts to more carefully examine the relevance and necessity of discovery requests, the aim of avoiding unnecessary time and costs in litigation is not always achieved. It would appear from the *Ryanair* case and recent decisions of the High Court and Commercial Court[166] that the old *Peruvian Guano*[167] test remains a criterion for discovery in Ireland. This may therefore allow discovery of material which may not necessarily be admissible in evidence, but which allows a party to advance its own case, or damage that of its opponent.

In order to obtain discovery of a particular category of documents, a party must demonstrate:

(a) that the documents in question relate to issues of fact upon which the applicant must succeed if she is to win her case, and

(b) that she will not be able to prove her case on this issue unless discovery of the documents is ordered.

Timing

Discovery traditionally tends to be called for at the close of pleadings, *i.e.,* after the delivery of the defence by the defendant and prior to the hearing itself, as at that stage it should be clear what the matters are that are in issue between the parties. In *Power City Ltd. v. Monahan (trading as Monahan Shipping),*[168] the timing of discovery was considered and in effect there should be "matters in issue" between the respective parties before discovery can be sought.

It is possible to apply for discovery earlier than at close of pleadings and even possible to do so prior to issuing proceedings. However, the success of such an application will generally require exceptional circumstances.[169] Particularly where an injunction is sought, discovery may be required at the interlocutory stage, or it may even be required before proceedings are commenced.

A party can also consider bringing an *Anton Piller* search order if it believes that essential documents may be about to be intentionally destroyed. However, the burden on the applicant is quite high and they would need to show (1) a strong prima facie case; (2) that the possibility of damage is very serious; (3) that the items are present and that there is a strong risk that they will be removed/destroyed before the trial; (4) that inspecting/removing the items will not damage the respondent's case; and (5) there is a heavy burden on the applicant regarding the undertaking as to damages and to preserve the items.

In *Fitzgerald v. PJ Carroll & Co. Ltd. & Anor*,[170] Mr. Justice Butler made an innovative order under Order SQ rule 5[171] of the Rules of the Superior Courts and pursuant to the inherent jurisdiction of the courts permitting a solicitor from each party to act jointly to inspect and take up copies of the plaintiff's lifetime medical records. This was not a discovery application, it was prior to any defence being delivered and was in the context of a real risk of the destruction of the medical records.

---

[165] In *Ryanair v. Aer Rianta Cpt.* [2003] 4 I.R. 264, the Supreme Court noted the new rules had shifted the burden of proof so that the applicant must discharge the prima fade burden of proving that the discovery sought "is necessary for disposing fairly of the cause or matter or for saving costs," Mr. Justice Fennelly stated in his judgment that: "Apart from this alteration of the prima face burden of proof, it is clear that the rule made no serious or fundamental change in the law regarding discovery of documents. The definition by Brett U (in *Compagnie Financiere du Pacifique v. Peruvian Guano Co.* (1882) 11 0.6.0. 55 at p. 63) remains the universally accepted test of what is the primary requirement for discovery, namely the relevance of the documents sought."

[166] *Schneider (Europe) GmbH v. Conor Medsystems Ireland Ltd.* [2007] IEHC 63 and *Medtronic Inc. & Ors v. Guidant Corp.* [2007] IENC 37.

[167] *Companie Financiere et Commerciale du Pacifique v. Peruvian Guano Co.* (1682) 11 080 55, CA.

[168] *Power City Ltd. v. Monahan (trading as Monahan Shipping)*, Unreported, High Court, Kinlan J, 14 October 1996.

[169] *Law Society of Ireland v. Rawlinson & Hunter* [1997] 3 I.R. 592.

[170] *Fitzgerald v. PJ Carroll & Co. Ltd. & Anor*, Unreported, High Court, 12 July 2001, Butler J, and similar orders in *CaIIery v. Benson & Hedges Ltd.* and *Morris v. Gallaher (Dublin) Ltd.* on the same date.

[171] Rule 5 of the Rules of the Superior Courts: "The court, by which any cause or matter may be heard or tried with or without a jury, or before which any cause or matter may be brought by way of appeal, may inspect any property or thing concerning which any question may arise therein."

In *Clarke v. Drogheda Corporation,*[172] the Master of the High Court, who hears the majority of discovery applications, set out questions that he suggested should be answered by a party seeking discovery:[173]

1 What are the facts in dispute?

2 Which of these are material, and which surplus?

3 What documents might lead to probative (and admissible) evidence concerning the disputed material facts?

4 Can I prove the disputed fact without discovery?

The fourth point has been touched on above and is perhaps of particular importance as it may be possible to prove the causal/material fact by some other means or obtain the documentation via another source like the Internet. Mr. Justice Fennelly in *Ryanair plc v. Aer Rianta Cpt.*[174] noted that documentation sought could be obtained by another means. In this regard, the potential cost of discovery vis-a-vis the other potential means could come into play.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Pre-Action Discovery

It is possible to obtain pre-action discovery, however this would not be the norm (see Timing section in question 2 above). One pre-trial avenue available is the *Norwich Pharmacal* order. This is an order that can be granted when the only relief sought is discovery and no other cause of action exists. Such an order was granted for the first time in the English case of *Norwich Pharmacal Co. v. Customs and Excise Commissioners,*[175] where the order was granted to enable the plaintiffs to identify the wrongdoers in order to bring proceedings against them. The availability of this form of relief was referred to by the Irish Supreme Court in *Megaleasing UK Limited & Others v. Barrett & Others.*[176] Though not commonly used in Ireland, it is an available means of obtaining pre-action disclosure from non-parties.

Non-Party Discovery

It is possible under Order 31 rule 29 of the Rules of the Superior Courts to obtain nonparty discovery.[177] However, like all discovery it is discretionary and given that it relates to nonparties, the courts apply an increased onus of proof on parties seeking non-party discovery. Order 31 rule 29 provides as follows:

> Any person not a party to the cause or matter before the Court who appears to the Court to be likely to have or to have had in his possession custody or power any documents which are relevant to an issue arising or likely to arise out of the cause or matter or is or is likely to be in a position to give evidence relevant to any such issue may by leave of the Court upon the application of any party to the said cause or matter be directed by order of the Court to answer such interrogatories or to make discovery of such documents or to permit inspection of such documents. The provisions of this Order shall apply mutatis mutandis as if the said order of the Court had been directed to a party to the said cause or matter provided always that the party seeking such order shall indemnify such person in respect of all costs thereby reasonably incurred by such person and such costs borne by the said party shall be deemed to be costs of that party for the purposes of Order 99.

[172] *Clarke v. Drogheda Corporation* [2003] I.E.H.C. 30 (16 January 2003).

[173] The Master of the High Court was drawing on *Brooks Thomas Ltd. v. Impac Ltd.* [1999] 1 I.L.R.M. 171 by examining the aspects that each party must prove in order to succeed and what documents are relevant.

[174] *Ryanair plc v. Aer Rianta Cpt.* [2003] 4 I.R. 264, at p.277.

[175] *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] A.C. 133.

[176] *Megaleasing UK Ltd. & Others v. Barrett & Others* [1993] I.L.R.M. 497.

[177] Prior to 1986, it was not possible to obtain an order for discovery against a non-party and the only way to obtain documentation from a non-party was by means of subpoena *duces tecum*, which could compel a non-party to produce certain documents or other evidence to the court at the trial of the action.

Voluntary non-party discovery must be attempted before seeking a court order unless the court decides that it is appropriate by virtue of the urgency of the matter, consent of the parties, other circumstances or the nature of the case to forgo this requirement. Non-party discovery is often, somewhat confusingly, referred to in practice as third party discovery.

If voluntary discovery cannot be agreed, a court order can be applied for. Parties must show on affidavit that: (1) it is likely that documents relevant to an issue in the action exist;[178] (2) the non-party is likely to have the documents in her possession, custody or power; (3) the identity of the documents is clear; (4) the documents are not available to the applicant otherwise then by means of a non-party discovery order;[179] and (5) an order is necessary for disposing fairly of the cause or matter or for saving costs.[180] The applicant will also be required to indemnify the non-party for all costs reasonably incurred by the non-party in complying with the order.

However, even if all of the above are established, the Court has an important further discretion to refuse the application if it considers that "particular oppression or prejudice will be caused to the person called upon to make discovery which is not capable of being adequately compensated by the payment by the party seeking discovery of the costs of the making thereto."[181]

Test for Non-Party Discovery

A helpful five-point test for non-party discovery was set out by Mr. Justice Costello in *Holloway v. Belenos Publications*:[182]

(a) the existence of relevant documents must be proven;

(b) it must be shown that these documents are in possession, custody or power of procurement of the party against whom discovery is sought;

(c) the court must be satisfied that in the circumstances, it is correct to exercise its discretion to order third party discovery;

(d) principles which we normally associate with inter partes discovery, *e.g.,* privilege, will apply;

(e) requirements of the rule as regards saving costs will apply.

Grounds for Refusing Non Party Discovery

1. *Public Policy*

   The courts can take public policy considerations into account in relation to non-party discovery applications. In *PMPS Ltd. v. PMPA Insurance plc.*[183] the plaintiff sought discovery of a memorandum prepared by the Registrar of Friendly Societies (a non-party) and correspondence between the Registrar and a government Department[184] regarding the relationship between the parties to the action. However, the court refused the application on the grounds that to make the order would be contrary to the public interest.

2. *Delay*

   Non party discovery should be sought as quickly as possible.[185]

3. *Court's Discretion*

   As with Inter-Partes discovery, numerous factors can influence how a court will exercise its discretion. For example, the object of the discovery must not be frivolous and the conduct and motivation of the applicant can be taken into account. Further, it may be considered oppressive to order production of a vast amount of documents of slight relevance. This list of factors is by no means exhaustive.

[178] *Holloway v. Belenos Publications Ltd.* (No. 1) [1987] I.R. 405.
[179] *In re National Irish Bank* [2006] 2 I.L.R.M. 263.
[180] *Allied Irish Bank plc v. Ernst & Whinney* [1993] 1 I.R. 375.
[181] Judgment of Mr Justice O'Donovan in *Ulster Bank Ltd. v. Byrne* [1997] J I.E.H.C. 120 (10 July 1997), referring to the Supreme Court's decision in *Allied Irish Banks Plc. and Allied Irish Banks (Holdings and Investments) Limited, Plaintiffs, v. Ernst & Whinney. Defendant, and The Minister for Industry and Commerce, Notice Party* [1993] 1 I.R. 37526.
[182] *Holloway v. Belenos Publications*, Unreported, High Court, 3 April 1987.
[183] *PMPS Ltd v. PMPA Insurance plc* [1991] I.R. 284.
[184] The Department of Industry and Commerce, as it then was.
[185] *Crofter Properties Limited v. Genport Ltd.*, Unreported, Supreme Court, 2 May 2000.

Non-Parties Outside the Jurisdiction

Applications for discovery against non-parties based outside the jurisdiction are even more narrowly construed by the courts. This issue was examined by the Irish Supreme Court in *Fusco v. O'Dea,*[186] which involved an application to join the government of the United Kingdom as defendants, or in the alternative to seek non-party discovery from them. The Supreme Court indicated that Order 31 rule 29 should be narrowly construed and refused the application. Mr Justice Egan stated in his judgment that:

> The wording of Order 31, rule 29 is silent as to the issue of its possible applications to third parties outside the jurisdiction. However, although the rule is drafted widely – the court may order any person having in his possession, custody or power relevant documents – it is arguable that it should be construed narrowly. Costello J adopted a restrictive approach when interpreting the rule in *Allied Irish Banks plc. v. Ernst & Whinney* [1993] 1 I.R. 375 (at p. 381): The onus is on the applicant to satisfy the court that such documents are in the notice party's power or possession. If it does not do so, the court has no jurisdiction to make an order.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The Statutes of Limitations[187] specify periods within which particular types of claims may be brought. For example, an action claiming damages in respect of personal injuries (except fatal) caused by negligence, nuisance or breach of duty must be brought within two years of the date on which the cause of action accrued, or (if later) the date of knowledge of the person injured. For other general tort claims and breach of contract claims the limitation period is six years, and it is twelve years for an action in relation to the recovery of land.[188]

Best practice is to keep the documents for at least a year after the limitation period set out in the Statutes of Limitations has expired, as a party has up to a year from issuing proceedings in the High Court to actually serve them on the defendant.[189] There are also statutory requirements for the preservation of specific types of records for certain time periods which must be observed, *e.g.,* in order to show compliance with tax regulations, company books and records requirements, anti-money laundering legislation, and employee working time regulations. Documents should only be destroyed where the relevant statutory regulatory periods have elapsed, there is no contemplated or existing relevant litigation and there is no further purpose in retaining the documents.

Section 18 of the Electronic Commerce Act mitigates to some extent the requirement to retain vast quantities of paper. Section 18(1) provides:

> If by law or otherwise a person or public body is required … or permitted to retain for a particular period or produce a document that is in the form of paper or other material on which information may be recorded in written form, then, subject to subsection (2), the person or public body may retain throughout the relevant period or, as the case may be, produce, the document in electronic form, whether as an electronic communication or otherwise.

Conversely, there are data protection and privacy requirements which impose obligations not to retain certain data after specific periods. For example, under the Data Protection Acts 1988 and 2003, data obtained for specified lawful purposes "shall not be kept for longer than is necessary for that purpose or those purposes."[190] This area can be further complicated where there are competing obligations, either due to contradictory international requirements, or due to the potential impact of data protection requirements and careful legal advice should be obtained.

---

[186] *Fusco v. O'Dea* [1994] 2 I.L.R.M. 389.

[187] The Statute of Limitations Act 1957, Statute of Limitations (Amendment) Act 1991 (as further amended by the Civil Liability and Courts Liability Act 2004) and Statute of Limitations (Amendment) Act 2000, may be cited as the Statutes of Limitations and shall be construed together as one Act.

[188] Unless the action for the recovery of land is being brought by the state, in which case the limitation period is 30 years.

[189] This may be further extended by the Court in certain circumstances.

[190] Section 2(1)(c)(iv) of the Data Protection Acts 1988 and 2003.

It is important to have clear document retention policies that follow industry and legal best practices in relation to document destruction and retention. Once these have been established, they should be carefully implemented and reviewed on a regular basis to ensure they continue to comply with best practices.

In the event of litigation or potential litigation it is important to seek legal advice as to any document retention requirements in relation to each specific case. Parties in litigation and their agents and advisers have a positive obligation to preserve documents and to provide proper discovery. Also, solicitors (as officers of the court) owe a separate duty to the court to take positive steps, as soon as litigation is contemplated, to ensure that their clients understand the importance of preserving documents which may have to be disclosed. Legal advisors should clearly explain the discovery process and the duty to retain all potentially relevant documentation and can, for example, co-ordinate sending out litigation hold notices to relevant people and areas within the organisation, in order to suspend normal document retention procedures.

The prudent approach is therefore that if there is a doubt, it is preferable to keep the potentially relevant document rather than allowing it to be destroyed in accordance with usual document retention requirements. Suspending a document retention procedure (or the relevant part of it) may have significant cost consequences in terms of additional storage requirements, so these requirements should be reviewed as the details of the claim along with the categories of documents that are likely to be relevant become clearer. Once assessed, it may be possible to allow certain document retention procedures to return to normal if they relate to documents that are beyond the scope of the litigation.

The manner in which documents are preserved is also important. Parties are obliged to discover and offer for inspection original documents. Originals should not be altered in any way. Staples, paper clips and post it notes are all potentially relevant and as such should be left in place for the purposes of discovery.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

Failure to preserve documents which are required for the purposes of the litigation can have serious consequences. Even fairly minor destruction of documents may adversely affect the case, lead to a loss of credibility with the court, or to the court drawing adverse inferences against a party. The defaulting party will be liable to attachment or the court may strike out a defendant's defence (or a plaintiff's claim if they were the relevant party).[191] An attachment order would involve the defaulting party being brought before the court to explain why they are in breach of the terms of the order. It could also result in criminal liability for perverting the course of justice where a court finds that the destruction amounted to a deliberate attempt to suppress evidence. Order 31 rule 23 specifically extends the potential liability to solicitors by providing that:

> A solicitor, upon whom an order against any party for interrogatories or discovery or inspection is served under rule 22, who neglects without reasonable excuse to give notice thereof to his client, shall be liable to attachment.

A party making discovery must set out on affidavit details of the documents that they had in their power or possession but which they no longer have. They must explain when they were last in their power or possession and what has become of them, or whose power or possession they are now in.

In October 2007 the Supreme Court[192] was asked to consider a perhaps related but different situation, where journalists from The Irish Times newspaper had deliberately destroyed documents that were unsolicited and anonymously provided to them, after receiving a summons from a Tribunal of Inquiry in relation to the documents. The journalists claimed public interest in the preservation from disclosure of journalistic sources as an essential prerequisite of a free press in a democratic society.[193] The Supreme Court considered this in context of the Tribunal's legal powers to conduct the inquiry and to summons the defendants. The Supreme Court stated:

> Against this background the deliberate decision taken by the defendants to destroy the documents at issue in this case after they had received a summons to produce these to the

[191] In accordance with RSC Order 31 Rule 21.
[192] *Judge Mahon v. Keena & Kennedy* [2007] IEHC 348.
[193] They also relied on their right to freedom of expression as guaranteed in Article 40.6.1.i of the Constitution, and Article 10 of the European Convention on Human Rights.

> Tribunal and after having taken legal advice, is an astounding and flagrant disregard of the rule of law.

The Supreme Court concluded that the journalists be directed to answer questions concerning the nature of the documents received by them as:

> The defendants' privilege against disclosure of sources, is overwhelmingly outweighed by the pressing social need to preserve public confidence in the Tribunal and as there is no other means, by which this can be done other than the enquiry undertaken by the Tribunal, we are of opinion that the test "necessary in a democratic society" is satisfied.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

The general rule for all costs is that they follow the event, that is, that the successful party is also awarded its costs against the unsuccessful party. Thus it should be ensured that the final order in a case takes the costs of any discovery applications into account. The costs arising from discovery applications must be certified by the court at trial for those costs to be allowed on taxation. If a case never comes to trial, but settles on the basis that the costs will be "taxed in default of agreement," *i.e.,* independently assessed by a Taxing Master, the Taxing Master can certify and allow discovery costs if he deems such a request reasonable.

The Costs of Non-Party Discovery

Order 31 rule 29 of the Rules of the Superior Courts deals with non-party discovery and provides:

> the provisions of this order shall apply mutatis mutandis as if the said order of the court had been directed to a party to the said cause or matter provided always that the party seeking such order shall indemnify such person in respect of all costs thereby reasonably incurred by such person and such costs born by the said party shall be deemed to be costs of that party for the purposes of Order 99.

The reasonably incurred costs of non-parties who are required to make discovery must be indemnified by the party seeking that discovery. The non-party is also generally entitled to their fees and expenses for having to comply with the order for discovery. Therefore, for example, an order against a non-party firm of auditors should entitle them to charge not just for their legal fees, outlay and VAT,[194] but also for their own time and expenses in carrying out the relevant discovery searches of their records. The costs borne by the party who sought the non-party discovery are deemed to be part of that party's overall costs for the purposes of Order 99.[195]

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

Superior Court rules require discovery of "documents" but provide no definition of what that is. However, its meaning has been developed through case law so as to include anything which contains information.[196] It therefore extends beyond written documents such as letters, minutes and file notes and extends to photographs, tapes, discs and electronically stored information. The Law Society of Ireland have recommended that this be put beyond doubt by amending Order 31 rule 12 so as to define "document" as "documents including electronically stored information."

There is no independent set of rules for electronic discovery and so the ordinary rules of discovery[197] apply. This means that for the moment at least, an order to disclose all documents in a particular category must

[194] Value Added Tax.
[195] Pursuant to RSC Order 31 Rule 29.
[196] *McCarthy v. O'Flynn* [1979] I.R. 127.
[197] RSC Order 31.

include data from all electronic sources, such as active data, metadata, replicate data and back-up data. In practice, parties tend to disclose only active data. This exclusion is without legal basis and arguably amounts technically to a breach of the discovery rules.

This status of electronic documents is reinforced by the Electronic Commerce Act 2000,[198] which provides for, *inter alia,* the legal recognition of electronic contracts, electronic writing, electronic signatures and original information in electronic form in relation to commercial and non-commercial matters. It also deals with admissibility of evidence and states that in any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility in evidence of an electronic communication, electronic form of document, an electronic contract or electronic signature.[199] This Act gave express legal recognition to storage of information in electronic format and set out detailed requirements as to the integrity of electronic information if it is to be used for this purpose. Section 9 provides that:

> information (including information incorporated by reference) shall not be denied legal effect, validity or enforceability solely on the grounds that it is wholly or partly in electronic form) whether as an electronic communication or otherwise.

As is the norm in our legal system, the courts have also made clear that they will develop the law to take account of new technological developments. In *Dome Telecom Ltd. v. Eircom plc.,*[200] Fennelly, J. stated that:

> failure by the courts to move with the times by adapting the rules to new technology might encourage unscrupulous businesses to keep their records in a form which would defeat the ends of justice.

The scope of discovery of electronic documentation was dealt with by Mr. Justice Clarke in the High Court in *Mulcahy v. Avoca Capital Holdings Ltd.*[201] Here, there were a series of allegations by both sides in relation to alleged improper uses of the defendant's computer facilities and the plaintiff sought a forensic examination of his employer's computers. The court allowed the plaintiff's computer experts have access to the PCs of two joint managing directors in order to determine whether they had opened documents that they would not normally have had access to and to ensure fair procedures in the litigation, but it also imposed conditions on this access to protect information that was confidential to the company. The defendants had no discretion in refusing the plaintiffs experts access to any relevant documentation.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

There is currently no definition of "electronic document" or "electronic data" for discovery purposes. However, "document" continues to be interpreted as including electronic documents and therefore electronic disclosure is taking place in any event. As discussed there has been a recommendation in October 2007 by the Law Society of Ireland[202] to define "document" as "documents including electronically stored information," but no such amendment has been made to date.

Over the years the definition of "document" has continued to need to evolve with developments in technology and use and it has been somewhat of a judicial challenge to continue to keep this current. The Supreme Court held in *McCarthy v. 0 Flynn*[203] that the word "document" should be construed so that it would "comprehend the full range of things which could become part of the court file at the end of the hearing of the proceedings" and in that sense would clearly include X-ray films. This suggests a flexible attitude will be adopted by the Irish Courts and there is nothing to suggest that the *dicta* of Mr Justice Vinelott in Derby, where he held that a computer database and information held on backup tapes are documents for the purposes of discovery, will not be followed[204] or even developed if necessary.

---

[198] Which was digitally signed by the Irish President, Mary McAleese, on 10 July 2000.
[199] Section 22 of the Electronic Commerce Act 2000.
[200] *Dome Telecom Ltd. v. Eircom plc.* [2007] IESC 59.
[201] *Mulcahy v. Avoca Capital Holdings Ltd.* [2005] IEHC 136 (14 April 2005).
[202] Law Society of Ireland — Civil Litigation Discovery in the Electronic Age: Proposals for Change; October 2007.
[203] *McCarthy v. 0 Flynn* [1979] IR 127.
[204] *Derby and Co. Ltd. v. We/don (No. 9)* [1991] 2 All ER 90. This dicta was referred to by Denham J in her judgment in *Keane v. Bord Pleanala* [1997] 1 IR 184.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

There are currently no specific requirements for parties to meet and discuss electronic discovery. However, as part of the pre-trial procedure for proceedings in the Commercial Court, a judge may at the initial directions hearing, of his own motion after hearing the parties, or on application of a party by motion or notice to the other party, give directions to facilitate the determination of the proceedings.[205] This includes directions providing for the exchange of documents or information between the parties on such terms and conditions as the judge may direct, which may also include electronically. Therefore it appears that while the subsection does not make express provision for the transmission between the parties of the information electronically, it remains within the competence of the judge in commercial proceedings to give a direction to that effect.[206] Provisions for the electronic filing and exchange of documents, electronic presentation of evidence, video conferencing and real-time stenography have been made.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

The same requirements from the statutes of limitations and other statutory and regulatory requirements would apply to electronic documents as apply to non electronic documents (see question 4 above). The Electronic Commerce Act 2000 provides for the electronic retention of documents by persons and public bodies and the production of electronic documents as evidence.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

There are currently no rules specific to electronic discovery of documents and therefore the same rules would apply as apply to paper documents. Parties must hand over relevant and necessary documents that are in their "possession, custody or power". As certain documents, *e.g.,* documents held by a person's bank, will be in their power though not in their physical possession, parties must ensure not to omit or overlook these documents when making discovery.

In Ireland, the obligation to search is extensive, as the obligation on parties is to give discovery of *all* documents within an agreed category. There are no allowances for the making of *proportionate* searches. This poses obvious potential for discovery to become unmanageable, especially in the context of electronically stored information. However, the courts have indicated that they will be willing in certain instances to limit the level of searching required. In *Dome Telecom Ltd. v. Eircom plc.*[207] the plaintiff sought discovery of extensive electronically stored data. The majority of the Supreme Court refused the application on the basis that they did not believe that "the likely benefit, if any" to the Respondent of obtaining "the…discovery was sufficient to justify the highly unusual and burdensome form of discovery sought."

The Law Society of Ireland have recommended that the rules be amended to expressly entitle the court to limit at any time the discovery agreed or ordered if satisfied that such limitation is justified in light of the cost and burden of searching for and providing such documents and the degree to which they are relevant and necessary.

Once all documents are compiled, they are set out in an affidavit. A party is entitled to serve notice on another party to produce for inspection documents referred to in their affidavit of discovery and the requesting party is entitled to take copies.[208] Order 31 Rule 15 of the Rules of the Superior Courts states:

> Every party to a cause or matter shall be entitled at any time, by notice in writing, to give notice to any other party, in whose pleadings, or affidavit or list of documents references is made to any document, to produce such document for the inspection of the party giving such notice, or of her solicitor, and to permit copies thereof to be taken.

[205] RSC Order 63A Rule 6(1).
[206] Under RSC Order 63A Rule 21(3), the Judge of the Commercial Court may direct that the trial booklet should be produced in electronic form and may further direct that it should be lodged or served by electronic means.
[207] *Dome Telecom Ltd. v. Eircom plc.* [2007] I.E.S.C. 59.
[208] RSC Order 31 Rule 15.

The court can make an order for inspection "in such place and in such manner as it may think fit"[209] subject always to the proviso that an order shall not be made if it is not necessary either for disposing fairly of the cause or matter or for saving costs.

The court may also order the production of any relevant entries in business books.[210] These must be verified by an affidavit setting out details of any erasures, interlineations or alterations and the court retains discretion to order inspection of the original books.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

Searching electronic documents is more technical in nature and usually involves more significant volumes and potentially higher costs than paper documents (*e.g.,* if legacy systems and back up tapes are involved). However, the same principles would apply in terms of the obligations on a party responding to any discovery request. The affidavit of discovery essentially verifies that all required searches have been made.

If there was any doubt as to the thoroughness of the search or documents produced, a letter should be sent to the defaulting party's solicitors pointing out the deficiency. In the absence of a satisfactory response, a court order can be sought to compel further and better discovery. Under Order 31 Rule 20 a party can be required to swear an affidavit stating whether specific documents are or have been in their possession, when they parted with the documents if not in their possession and what has become of the documents in question.

Further, if a document has not been produced at the discovery stage, the defaulting party cannot rely on it at trial,[211] at least in the absence of a reasonable explanation as to why it was not disclosed on time. Thus it is often in a party's best interests to make comprehensive searches at the time of making discovery.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

The Rules of the Superior Court provide no specific rules as to how electronic documents should be produced, so at present the rules as regards any discovery apply. Thus, electronic documents should be produced in such manner that they can be both inspected and copied by the other side. There is no existing right to receive electronically stored information in a searchable form, despite the ease this could bring to the process. The Law Society of Ireland has recommended that the rules be amended so as to require the provision of electronic documents in searchable form on two conditions: (1) that it is held in that form by the party giving the discovery, and (2) that it can be provided in that form without significant cost to the party providing the discovery.

The courts have shown willingness to develop rules regarding production as and when the circumstances require. In *James McGrath v. Trintech Technologies Ltd. and Trintech Group PLC*,[212] the plaintiff was required to hand over laptops to an independent expert who would reconstitute the documents contained on their hard drives and make hard copies of the documents. The court ruled that the expert was not to be contacted by the defendant, except in relation to fees.

Under the current rules, the Notice to Produce Documents[213] requires the applicant to describe the documents to be produced and does not make reference to the form in which they are to be produced. Section 22 of the E-Commerce Act 2000:

> nothing in the application of the rules of evidence shall apply so as to deny the admissibility in evidence of (a) . . . an electronic form of a document . . . on the sole ground that it is fin electronic form] . . . or (b) if it is the best evidence that the person . . . adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

[209] RSC Order 31 Rule 18.
[210] RSC Order 31 Rule 20(1).
[211] *Bula Limited (in receivership) and Others v Lawrence Crowley*, Unreported, High Court, 19 December 1989.
[212] *James McGrath v. Trintech Technologies Ltd. and Trintech Group PLC,* The High Court – 2003 10331P.
[213] As set out in RSC Appendix C Form 11.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

There are currently no specific standards particular to electronic information. The same requirements would apply as with paper and other non-electronic documents (see above). Care should be taken not to alter original electronic documents in any way prior to making discovery.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

The traditional common law approach was that disclosure of privileged communications, whether by inadvertence or misconduct, resulted in the loss of the privilege and evidence of the privileged communications. Where privileged information is inadvertently disclosed it may be possible to convert the mistake. While it depends on the circumstances, if no inspection has taken place but if the documents have been incorrectly listed in the affidavit of discovery and included among the non-privileged documents that can be rectified either by agreement or by the filing of a supplemental affidavit. However, if inspection has taken place, the general rule is that privilege is deemed to be waived and it is too late to correct the mistake because the substance of the document has been communicated to the other side. The same rules would apply to both electronic and non electronic documents.

This general rule is not absolute, however, and the courts may uphold a claim to privilege where documents have been disclosed in certain circumstances. Generally, the following two stage test is applied by the courts; (1) whether it was evident to the solicitor receiving the documents that a mistake had been made, and (2) whether objectively it would have been obvious to a hypothetical reasonable solicitor that disclosure was inadvertent. The "reasonable solicitor" approach has been taken in a number of cases.[214]

There are two classes of documents that are privileged from disclosure: (a) legal advice privilege, and (b) litigation privilege. Legal advice privilege includes any confidential communications to or from a lawyer for the purpose of obtaining or providing legal advice. Litigation privilege extends to all documents created during or in contemplation of litigation, including communication between lawyers or their clients and third parties, provided the dominant purpose of the communication is to assist in the litigation. In relation to documents created prior to proceedings being issued, the courts will consider the extent to which litigation was "in contemplation." For example, in *Power City Ltd. v. Monahan (t/a Monahan Shipping)*,[215] the High Court held that privilege existed in relation to correspondence which was subsequent to the threat of proceedings by the plaintiff and also on the basis that this correspondence would have had no reason to exist other than for the purpose of preparing a defence.

Legal privilege in Ireland belongs to the client and attaches to the document, rather than a person, and it can be waived. Provided the document fulfils the conditions for attracting privilege under either of the two bases set out above, the document is privileged in the hands of the lawyer or client. Privilege can also be asserted over communications between different lawyers acting for clients with a common interest, such as co-defendants.

Sending Privileged Documents Cross-Border

If privileged documents are sent to another jurisdiction where they are not covered by privilege, this would reduce the chances of making a successful claim of privilege in Ireland. If it is necessary to do so, they should at least be clearly marked as privileged and circulation should be kept to a minimum. If privileged documents are being sent to a court or regulator in a foreign jurisdiction where they will not be covered by privilege, there is a risk that this could be seen as a waiver of privilege in Ireland. However, the first position has to be that privilege will be maintained in such circumstances. If the document is made publicly available in another jurisdiction and therefore loses confidentiality, it will also be difficult to make a valid assertion of privilege in Ireland.

[214] *Shell E&P Ltd. v. McGrath* [2006] IEHC 409, *Byrne v. Shannon Foynes* [2007] IEHC 315.
[215] *Power City Limited v. Monahan (t/a Monahan Shipping)* [1996] 1 EHC 22(14 October 1996).

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

The costs of electronic information discovery are dealt with under the same provisions as non-electronic discovery costs (as detailed above) and there are currently no specific rules in relation to the costs of electronic discovery. The courts have indicated a willingness to adapt existing rules in order to meet the requirements of developing technology.

This is evident from *James McGrath v. Trintech Technologies Ltd. and Trintech Group PLC*[216] where O'Sullivan, J. ordered the plaintiff to produce "...emails, instantaneous messages (Yahoo), logs etc.…all entries…in the plaintiff's electronic diary including emails to himself and others, instantaneous messages (Yahoo), logs etc." However, the defendants were required to instruct and pay for an independent expert to do the following: (1) Reconstitute the documents contained on hard drives of the two company laptop personal computers which are the property of the defendant companies herein but which are currently in the possession of the plaintiff, (2) Make hard copies of the said documents and send them with the two said laptops to the plaintiff's solicitor. The defendant was further required not to communicate with the independent expert save to discharge his fees.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

Prudent parties would have information and document management policies which include records retention schedules and details of how legal hold notices are to be used to ensure the preservation of electronic information for business and legal purposes. Data Protection issues would also apply to any personal data. There are recommendations by various professional bodies to their members, *e.g.,* the Law Society published a general guidance note,[217] which provides that all electronic storage of documentation should be for at least the same period as would apply to the paper version. They note that 3 key issues affecting electronic storage are: (1) permanency or durability of the format; (2) accessibility of the format; and (3) security of the format.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The use of electronic information management technologies to assist with the preservation, classification, and management of electronic information for legal reasons is continuing to grow in Ireland and would be more prevalent amongst large national and multinational corporations with significant levels of documents that in smaller businesses.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

There is an unenumerated right to privacy under Article 40.3.1 of the Irish Constitution, an explicit right under article 8 of the European Convention on Human Rights and EU Data Protection Directives as implemented by the Data Protection Acts 1988 and 2003. These would apply equally to electronic documents. (See also questions 20(a) and 20(c) below).

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

    a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

    The right to privacy under Irish law is drawn from a human right to privacy, an unenumerated right to privacy under Article 40.3.1 of the Irish Constitution, an explicit right under European Convention on Human Rights and EU Data Protection Directives.

[216] *James McGrath v. Trintech Technologies Ltd. and Trintech Group PLC*, The High Court – 2003 10331P.
[217] Law Society Guidance Note on the Retention or Destruction of Files and Other Papers and Electronic Storage.

Article 40.3.1 of the Irish Constitution provides that: "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens."

The Irish Supreme Court held in *McGee v. Attorney General*[218] that there is an unenumerated (implied) right to privacy (in this case marital privacy). However, in *Norris v. Attorney General,*[219] the Supreme Court held that "A right of privacy or, as it has been put, a right "to be let alone"[220] can never be absolute." In *Kennedy and Arnold v. Ireland,*[221] the Supreme Court held: "The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State." Article 8 of the European Convention on Human Rights Act 2003[222] deals with the right to respect for private and family life.

1. The Data Protection Directive 95/46/EC was implemented in Ireland by Data Protection Acts 1988 and 2003, The Electronic Privacy Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector was implemented by the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.[223] The purpose of the 1988 Act is to give effect to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and to regulate in accordance with its provisions the collection, processing, keeping use and disclosure of certain information relating to individuals that is processed automatically. The 2003 Act provides more stringent data protection measures and it has far reaching and important implications for business organisations which capture and deal in information leading to living individuals, in particular, customers and employees.

2. The Data Protection Acts establish a regulatory framework that governs the processing of personal data and which encompasses:

3. A requirement to adhere to certain "Data Protection Principles" in the collection, processing, keeping, use and disclosure of personal data;

4. A requirement that any processing be "legitimate," that is, that any processing must not only comply with the Data Protection Principles but must also come within one of a limited number of specified conditions and, in the case of "sensitive" category Personal Data, must come within an additional set of specified conditions;

5. A requirement that the data subject be provided with certain information concerning the processing of their personal data not only in situations where the information is directly obtained from the data subject but also in situations where it is obtained indirectly;

6. Specific requirements dealing with direct marketing;

7. Legal rights for individuals entitling them, *inter alia*, to establish the existence of personal data; access that personal data and have incorrect or inaccurate data rectified; blocked or erased; and certain rights in respect of automated decision making processes;

8. Certain controls on the transfer of personal data outside the EEA;

9. A duty of care that is owed by data controllers and data processers towards data subjects; and

10. A requirement that certain data controllers and data processors must register with the Data Protection Commissioner.

[218] *McGee v. Attorney General* [1974] IR 284 – an implied right to marital privacy.
[219] *Norris v. Attorney General* [1984] IR 36.
[220] This was a reference to the definition by Brandeis J of the United States Federal Supreme Court.
[221] *Kennedy and Arnold v. Ireland* [1987] IR 587.
[222] Article 8 provides that: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
[223] SI 535 of 2003.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

"Personal data" is defined by section 1(1) of the Data Protection Acts as:

> data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Therefore, the term "personal data" has a different meaning to the term "personal information" which is used in the Freedom of Information Acts 1997 and 2003 which refers to information that would in the normal course of events only be known to the individual, their family or friends or is held by a public body on the understanding that it is confidential.

"Sensitive personal data" is defined[224] as:

> personal data as to:
>
> (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
>
> (b) whether the data subject is a member of a trade-union,
>
> (c) the physical or mental health or condition or sexual life of the data subject,
>
> (d) the commission or alleged commission of any offence by the data subject, or
>
> (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings,
>
> and any cognate words shall be construed accordingly.

"Processing" effectively includes every conceivable use of information, including storing and filing and is defined[225] as:

> of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including:
>
> (a) obtaining, recording or keeping the information, or data,
>
> (b) collecting, organising, storing, altering or adapting the information or data,
>
> (c) retrieving, consulting or using the information or data,
>
> (d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
>
> (e) aligning, combining, blocking, erasing or destroying the information or data.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

The term "processing" incorporates "disclosure" and the combined effect of the Data Protection Principles is to impose a restriction on the disclosure of personal data in a manner which is incompatible with the purpose or purposes for which the personal data was originally obtained.

[224] Section 1(1) of the Data Protection Acts 1988 and 2003.
[225] Section 1(1) of the Data Protection Acts 1988 and 2003.

However, under the Data Protection Acts, any restrictions on the disclosure of personal data do not apply if the disclosure is:

1. in the opinion of senior officers of the Irish police or defence forces required for purposes of safeguarding the security of the State;
2. required for the purposes of preventing, detecting or investigation of offences, apprehending or prosecuting offenders or accessing or collecting any tax duty or other monies owed or payable to the State;
3. required in the interests of protecting the international relations of the State;
4. required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
5. required by or under any enactment, rule of law or order of a court;
6. required for the purpose of obtaining legal advice or for the purposes of, or in the course of legal proceedings in which the person undertaking the processing is a party or a witness; and
7. made at the request of or with the consent of the data subject or a person acting on his/her behalf.

A court may decide, for example, for confidentiality reasons, to limit production to a party's experts or legal team, without allowing access to the party directly. The courts will also limit information to the public in certain circumstances, *e.g.,* in some family law matters, matters relating to minors whereby they may be held in camera or the court may set parameters in relation to what journalists can report and protect the identities of certain parties.[226]

The main privacy rule which will impact on production of documents is privilege. This would apply to all forms of documents, including electronic documents and privilege can of course be waived. Private privilege has been held to attach/arise in a number of circumstances, including in relation to (1) privilege against self-incrimination; (2) marital privilege; (3) legal professional privilege; (4) litigation privilege; (5) without prejudice communications between the parties with an aim to compromise/settle the case.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

The Data Protection Acts are applicable both in the context of civil and criminal proceedings. However, as outlined above, a number of exemptions in the legislation may permit the disclosure of personal data in connection with such proceedings depending on the circumstances.

Rules regarding privilege can impact on the production of documents in civil matters, as discussed above. A duty to disclose in criminal proceedings arises on the basis that it is recognised that a defendant is entitled to have advance notice of the case made against her derived from the constitutional right to a fair trail. The Irish courts prefer an ad hoc approach in determining what should and should not be disclosed depending on the circumstances of each case.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

The Data Protection Acts 1988 and 2003 apply to the personal data of living individuals and the legislation establishes a number of legal rights for such individuals. This does not extend to legal entities such as a company as they are not individuals. If a company is established in Ireland and processes personal data, the legislation will apply to their business.

[226] The Supreme Court has held in *Goodman Int'l v. Mr. Justice Hamilton* that a tribunal of inquiry does not involve the administration of justice. Therefore, the constitutional requirement to have the proceedings heard in public imposed by Article 34.1 in respect of court proceedings does not apply.

Privacy rights may apply to legal persons as well as natural persons in certain circumstances. For example, companies can avail of legal professional privilege although marital privilege would of course not apply.

The rights granted to individuals by the Data Protection Acts include:

1. the right to establish the existence of personal data. This is the right to be informed by a person whether the person keeps any personal data relating to them and to be given a description of the data and the purposes for which they are kept;
2. the right of access to personal data. This is the right to be supplied with a description of the categories of data being processed by or on behalf of the data controller; the personal data constituting the data of which that individual is the data subject; the purposes of processing; the recipients or categories of recipients to whom the data are or may be disclosed and also to have communicated in intelligible form, the information constituting any personal data which the individual is the data subject; any information known or available to the data controller as to the source of those data and to be informed free of charge of the logic involved in any processing by automatic means of data of which the individual is the data subject where such processing constitutes or is likely to constitute the sole basis for any decisions significantly affecting him or her;
3. the right of access to examination results;
4. the right of rectification or erasure. This is the right to have rectified or where appropriate blocked or erased any data in which there has been a contravention of the Data Protection Principles;
5. the right to object to processing likely to cause damage or distress; and
6. certain rights in respect of the use of automated decision making processes.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

Compliance with data protection law is mandatory and non-compliance can lead to the Data Protection Commissioner issuing Information Notices, Enforcement Notices, Prohibition Notices; a court imposing fines or ordering that data material connected with the commission of offences is forfeited or destroyed and any relevant data erased.

Also non-compliance can result in adverse publicity through media reporting or publication by the Data Protection Commissioner of the matter on his website or in his annual report.

However, there are a number of exemptions provided for in the Data Protection Acts. For example, there are exemptions as follows:

1. Complete exemptions;
2. Exemptions from compliance with the Data Protection Principles;
3. Exemptions from compliance with the "legitimate processing" requirements;
4. Exemptions from the fair processing obligations to provide specific information to data subjects;
5. Exemptions from the data subject access provisions;
6. Exemptions from the provisions concerning the data subjects right to object to processing likely to cause damage or distress;

7. Exemptions from the provisions dealing with automated decision making processes;
8. Exemptions from restrictions on processing;
9. Exemptions from the transfer prohibition provisions; and
10. Journalism, literature and Art related exemptions.

See also paragraph (c) above.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

The Data Protection Acts apply in respect of "personal data." The Data Protection Acts make a distinction between "non-sensitive" and "sensitive" category personal data. The requirements of the Data Protection Acts are more restrictive as regards "sensitive" category personal data.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

Under the Data Protection Acts much employee related processing can be "legitimised" on the legitimate processing grounds that it is necessary for the performance of the employment contract or it is necessary for compliance with employment related legal obligations or it is necessary for the purposes of the legitimate interests of the employer. However, in the case of "sensitive" category personal data, the "legitimate processing grounds" are quite restrictive. While the Data Protection Acts enable consent (explicit consent on the case of sensitive personal data) to be used as a legitimate processing ground, the Data Protection Commissioner in the case of sensitive category personal data cautions against reliance on employee consent for such processing and emphasises that any such consent has to be "informed and freely given." This would mean that such consent would have to be capable of being withdrawn.

Recruitment and Selection

The collection of personal information during the process of recruitment gives candidates rights and imposes duties on employers. Employees and/or unions can also use the Data Protection Acts rights as a tool to gather information to support a claim under other legislation. Employers need to be aware of the need to justify requests for information sought from applicants. The Employment Equality Acts 1998 and 2004 highlight the importance of only seeking personal data that is relevant to the recruitment decision.

An important factor here also is the length of time that information concerning recruitment and non-recruitment is maintained by the employer.

Employment Records

Frequently many of the records that are required to be kept by employers arise as a result of employment law related obligations. Generally there is no data protection issue as regards those records. However, to the extent that such records go beyond what is required to be kept by law, then the issue turns on the extent to which the keeping of such records is in accordance with the Data Protection Principles and satisfies the "legitimate processing" requirements.

Sensitive Personal Data

The Data Protection Acts make a distinction between "non-sensitive" category personal data and "sensitive" category personal data (see (b) and (g)). The "legitimate processing conditions" that must be satisfied in the case of the processing of "sensitive" category personal data are more restrictive than those conditions that apply to the processing of "non-sensitive" category personal data.

An issue that is becoming increasingly topical concerns the use of biometric systems. The Data Protection Commissioner has prepared a guidance note in relation to employers seeking to use Biometric Systems in the workplace.[227] Before an employer installs a biometric system, the Data

[227] http://wwwdataprotection.ie/viewprint.asp?fn=/documents/guidance1bio.htm.

Protection Commissioner recommends that a documented privacy impact assessment is carried out. An employer who properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 and 2003, This is important, as a contravention may result in action being taking against an employer by the Commissioner, or could expose an employer to a claim for damages from an employee.

Extent of Right of Access

Please refer to question (e).

The Irish Data Protection Commissioner has ruled that a request for access must be answered no matter "how inconvenient or disagreeable" it is to a data controller unless the statutory restriction applies. Employers are no exception to this rule. While employers are not legally required to have a subject access procedure, they should consider having one in order to ensure and provide evidence of compliance with good employment practice and fairness to the individual.

Monitoring and Surveillance

Monitoring and surveillance is a particularly complex area as it raises issues of not only privacy and data protection but also telecommunications legislation (in the context of telephone intercepts). The Data Protection Commissioner accepts that in certain circumstances employers have legitimate interests to protect their businesses and that the legitimate interests can in certain circumstances include the deployment of monitoring and surveillance. However, any monitoring and surveillance has to be proportionate. The Data Protection Commissioner emphasises prevention rather than detection.

Employers should have clear policies setting out what is expected in relation to email, Internet, telephone and other IT usage, that the policies are actually followed and updated where necessary. Employers should ensure employees are fully aware of the policies as these impact on privacy rights they may have. Emails can include or comprise personal data and therefore employees may be entitled to access emails about them. This obviously has huge practical issues for employees faced with access requests. While advances in technology have increased the risks to an employer through misuse of email and Internet access by employees, technological advances also mean that it is much easier for an employer to monitor employees and there is a potential increased risk of intrusion in to private communications and activities, normal data protection principles apply to information collected by monitoring or surveillance. Therefore monitoring and surveillance would generally require the consent of individual employees or need to be permitted on one of the other grounds on which processing is permitted, *e.g.,* to prevent or detect crimes or to protect employer's legitimate interests. Monitoring generally needs to be undertaken for specified and legitimate purposes which are made clear to the employee.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The Irish regulatory agency for data protection is the Office of the Data Protection Commissioner.

All data controllers and data processors are required to register with the Office of the Data Protection Commissioner unless they are specifically exempted or specified by the Minister for Justice, Equality and Law Reform by ministerial regulation as not being required to register. For example, banks and financial/credit institutions; insurance undertakings; entities whose businesses consist solely or mainly of direct marketing, providing credit references or collecting debts; internet access providers; persons processing genetic data or data processors who process personal data on behalf of any of the foregoing are required to register.

As regards notification to data subjects, the general requirement here is the Data Protection Principle that data be obtained and processed fairly. This generally means that certain information has to be provided to a data subject concerning the processing of their data. The information to be provided differs depending on whether the data was obtained directly by the employers (in such

case, the information to be included includes the identity of the employer; the purpose or purposes which the data are intended to be processed and any other information that having regard to the specific circumstances is required to render the processing fair such as, *e.g.,* information as to the recipients or categories of recipients of the data; whether replies to questions asked are obligatory and the possible consequences of failure to give replies as well as the existence of the right of access to and the right to rectify the data).

In the case of data that has been indirectly obtained, the employer should provide the following additional information: the categories of the data concerned and the name of the original data controller. This information should be provided not later than the time when the employer first processes the data or if a disclosure of the data to a third party is envisaged, not later than the time of such disclosure.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

Generally, the main requirements are to ensure that the processing of the information for such purposes is done in accordance with the requirements of the Data Protection Acts, the most notable in this context being, the requirements to:

1. comply with the Data Protection Principles;
2. ensure that the processing comes within one of the applicable "legitimate" processing grounds (noting that the grounds are more restrictive in the case of "sensitive" category personal data);
3. that the data subject has been provided with the information necessary to ensure that the data has been fairly obtained and processed; and
4. where personal data is to be transferred outside the EEA that such transfer fulfils one of the conditions specified in the Data Protection Acts.

To the extent that data processors or other third parties are engaged by the data controller to assist in the processing of such information, the data controller has to ensure that such processing is carried pursuant to a contract in writing (or other equivalent form) which provides, *inter alia*, that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with security obligations equivalent to those imposed on the data controller by the Data Protection Acts. The data controller is required to ensure that any such data processor provides sufficient guarantees in respect of the technical security measures as well as organisational measures in respect of such processing.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

Please see question (h) above.

Under the Data Protection Acts, consent is recognised as one of the "legitimate" processing grounds both for "non-sensitive" and "sensitive" category personal data. However, the Irish Data Protection Commissioner follows the views of the Article 29 Working Party with regard to the use of the consent of the employee for the purposes of legitimising any processing of employee related data particularly in the case of "sensitive" category personal data. The view of the Data Protection Commissioner is that employers should seek to legitimise their processing of employee related data on grounds other than consent and that where the consent ground is used, that such consent has to be "informed and freely given." In essence this means that such consent must be capable of being withdrawn by the employee.

Accordingly, where the consent of the employee to processing has been obtained, the form of consent should provide sufficient relevant detail in relation to what personal data (including sensitive personal data) is to be processed, by whom and at the extent of which this maybe transferred outside the jurisdiction. This could include, for example, an explanation that the payroll function has been outsourced by the employer to a company in another jurisdiction.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Ireland is not a party to The Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters.[228] It is however a party to the Vienna Convention of 1961. The legislation governing the taking of cross border evidence and discovery in this jurisdiction consists of the Foreign Tribunals Evidence Act 1856 ("the 1856 Act") and Council Regulation (EC) No 1206/2001 ("the Regulation") on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

Irish courts may direct the taking of evidence in aid of non EU cross border proceedings pursuant to the 1856 Act. However the Irish courts construe this power strictly and will not entertain requests that solely amount to the discovery of documents.[229] Evidence under the act may be taken when a foreign court issues a Letter of Request (Letter Rogatory). Witnesses can only produce documents which touch upon their oral testimony. Countries who are also party to the Vienna Convention 1961 may be able to obtain certain documents pursuant to Article 5(j). This provides that consular functions consist in:

> transmitting judicial and extra judicial documents or executing letters rogatory or commissions to take evidence for the courts of the sending state in accordance with international agreements in force, or, in the absence of such international agreements, in any other matter compatible with the laws and regulations of the receiving state.

The position within the EU does appear to be broader. Article 1 of the Regulation which sets out its scope also refers solely to the taking of evidence, and not to the discovery of documents. However, Article 4, which deals with the form and content of evidence requests, elaborates on this somewhat. Article 4(f) requires that the requesting party give details of documents to be inspected where the request is for the taking of evidence in a form other then the examination of the person. This would appear to cover requests that are solely for the discovery of documents.

Letters of Request (*i.e.,* letters rogatory or commission rogatoire) are used pursuant to the Regulation. These are formal requests from one court to a foreign court, in this case for the disclosure of documents. Order 39 rule 5 of the Rules of the Superior Courts was amended by SI 13 of 2007: Rules of the Superior Courts (Evidence) 2007, which came into operation on 13 February, 2007. The new regime provided for a relatively simple and straightforward process and clarifies the bases upon which requests may be refused. It also provides certainty in the timing of the process by setting out specific timetables which apply.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

Ireland does not have any specific blocking statute, however, there is perhaps potential scope for the Irish Constitution or public policy reasons to be called upon.

---

[228] Although Ireland is party to *The Hague Convention on the Service Abroad of Judicial and Extra Judicial Documents in Civil and Commercial Matters*. The Master of the High Court is the relevant Central Authority in Ireland under the Service Convention. Within the European Union, the service of documents is governed by EC Regulation No. 1348/2000 on the service of judicial and extra judicial documents in civil or commercial matters, which came into force on 31 May 2001. However, from 13 November 2008 Regulation 1348/2000 will be repealed and replaced by EC Regulation 1393/2007.

[229] In Re *an Air Crash in the Florida Everglades on 11 May 1996* [1999] 2 I.R. 468.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The major factor considered in deciding whether to permit cross-border discovery is the jurisdiction of the requesting party. If they are a party to Council Regulation (EC) No 1206/2001 (namely all EU member states except Denmark), cross border discovery will be permitted in accordance with the Regulation and with Order 39 rule 5 of the Rules of the Superior Courts which was amended by SI 13 of 2007 (Rules of Superior Courts (Evidence) 2007). Even those in countries which are a party the regulation will only be permitted discovery on full compliance with Article 14. This provides that discovery will not be permitted if:

(a) the request does not fall within the scope of Article 1;

(b) the execution of the request is outside the functions of the judiciary in the requested member state;

(c) the requesting court does not comply with stipulated time limits;

(d) a deposit or advance requested under Article 18(3) is not made in time.

Further, pursuant to section 1(3) SI 13 of 2007 the Court may require the requesting party to file certain forms in the Central Office together with a certified translation thereof, and may also require an undertaking to reimburse fees before the discovery will be permitted.

For those countries outside the EU and Denmark, there is no legislation permitting cross border discovery in this jurisdiction. Letters of Request (*i.e.,* commission rogatoire or letters rogatory) are used in relation to these countries.

Netherlands

Jolling K.de Pree - ***Lead Editor***
Jan Pieter Hustinx, Tobias Cohen Jehoram, Lokke Moerel - ***Contributing Editors***
Wolter Wefers Bettink, AnneMarie Patberg - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

The Netherlands has a civil law system, the applicable rules of which are laid down in the Code of Civil Procedure (*Wetboek van Burgerlijke Rechtsvordering*). The organizational rules in regard of the judicial system are laid down in the Judiciary (Organization) Act (*Wet op de Rechterlijke Organisatie*).

The Dutch civil court system has three levels: the district courts, the courts of appeal and the Supreme Court.

District Courts

The Netherlands is divided into 19 districts, each with its own district court (*rechtbank*). The district courts have jurisdiction to hear any dispute which is of a civil law nature, although there are certain exceptions to this general rule. Each court is divided into several sector-specific chambers. These always include the administrative sector, civil sector, criminal sector and sub-district sector. Each chamber consists of three judges, although it is standard that certain hearings are held before one judge only. Applications for interim measures have to be brought before the president of the district court. Such applications can be brought without a corresponding main action.

In cases where the courts in several districts have territorial jurisdiction it is possible to bring actions before the courts in several districts simultaneously. A party involved in simultaneous procedures on the same subject matter can, however, request a transfer of the later case to the court where the same matter was already pending previously. In practice, no applicant will bring parallel actions before different district courts on the same subject matter, as the law to be applied by the courts is the same throughout the country and obtaining two identical or even conflicting judgments does in principle not make sense.

Courts of Appeal

The 19 districts are divided into five areas of Court of Appeal jurisdiction. There are thus five courts of appeal (*Gerechtshoven*). The courts of appeal are each divided into several chambers. Each chamber consists of five members. Courts of appeal do not only re-examine the legal merits but also the facts of the matter in full. In addition to criminal and civil cases, the courts of appeal also deal with all appeals against tax assessments, in their capacity as administrative court.

Supreme Court

The highest court in the country is the Supreme Court of the Netherlands (*Hoge Raad*) in The Hague, which hears appeals from the courts of appeal. The Supreme Court does not re-examine the facts of the matter. It may only set aside a judgment rendered by the courts of appeal, if it feels the law has not been applied properly or essential procedural rules have not been complied with. The chambers of the Supreme Court consist each of

five judges. The Supreme Court will give its ruling after the advocate general has submitted his advice on issues of law relevant to the case. The Supreme Court usually follows this advice.

Pre-trial discovery procedures similar to the U.S. procedures are not available in the Netherlands. The district courts and courts of appeal do, however, have the statutory possibility to order a party to make its books available for inspection, as well as to submit documents relevant to the case. Although parties are not obliged to comply with such orders, the courts are free to draw conclusions based on such refusal.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

As stated in our answer to question 1, pre-trial discovery procedures similar to those applicable in the U.S. are not available in the Netherlands. The district courts and courts of appeal do, however, have the possibility at any stage during the proceedings to order a party to make its books available for inspection (Article 162 of the Code on Civil Procedure ("CCP")), as well as to submit documents relevant to the case. Although parties are not obliged to comply with such orders, the court is free to draw conclusions based on such refusal.

Any interested party may request pre-trial hearings of parties and witnesses or pre-trial expert opinion for the purpose of gathering evidence. The party must state the nature and amount of the claim, the facts it aims to prove, the identity of the witnesses and the identity of the opposite party. The requesting party is under no duty to pursue the case after (unsatisfactory) pre-trial hearings.

Pursuant to Article 843a CCP, any party showing a legitimate interest may request a court to order a third party to submit documents with respect to a legal relationship to which the requesting party is a party. The documents should be identified by the claimant with a reasonable degree of precision. Third parties must comply with the order, unless legal privilege(s) or compelling reasons apply. To prevent fishing expeditions, the court needs to test the requesting party's legitimate interest. In short, in order to qualify for an order to submit documents pursuant to Article 843a CCP three cumulative conditions must be fulfilled:

(i) *Legitimate interest*: a party must argue and prove that it has a legitimate interest in disclosure. A legitimate interest is generally assumed if the requested documents are necessary to prove facts the requesting party has stated in pending litigation;

(ii) *Specified:* the requested disclosure should relate to specific – named – documents, *i.e.,* the documents should be identified and individualized;

(iii) *Legal relationship:* the requested documents must relate to a legal relationship to which the requesting party is party. Even though generally the documents must be of interest to the legal relationship between the requesting and the requested parties, documents can be subject to a third party relationship.

To secure this potential evidence, it is possible to make an attachment over these documents on the basis of the same article of the CCP.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

There is not as such a right to obtain disclosure either before or during proceedings from a non-party. However, such evidence may be gathered in the context of a pre-trial hearings of witnesses (see our answer to question 2), to the extent that a request to that effect is granted.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

   Under Dutch civil procedure, parties are at freedom to decide which evidence they submit and which not. However, parties are bound to present the required facts in full and according to the truth. If parties do not fulfill this obligation, the court is free to draw conclusions. As stated earlier (see our answer to question 2), it is possible for the courts to order a party to provide further specific information by – for instance – submitting documents. A party can only refuse to do so on the basis of compelling reasons. A party can request the court to order another party to submit specific documents, which are relevant to the case. There is no general statutory obligation to preserve documents for the purpose of legal proceedings.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

   See our answer to questions 2 and 4. Although there is no obligation to preserve documents for the purposes of litigation, and hence no sanction when a party fails to do so, a court can draw conclusions from the failure of a party to disclose all (or specific) evidence and materials in its possession.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

   In terms of Article 843a CCP, the costs of disclosure pursuant to that provision are for the party requesting the disclosure of the documents.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

   There are no specific rules or case law in regard of electronic disclosure. However, Article 843a CCP (see our answer to question 2) also applies to information stored on a data carrier.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   There is no specific definition of "electronic document" or "electronic data" for disclosure purposes.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

   No such legal provisions or general rules exist.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

    No such legal provisions or general rules exist.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

    No such legal provisions or general rules exist.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

    No such legal provisions or general rules exist.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

    No such legal provisions or general rules exist.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

    Not applicable (see our answer to question 7).

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

    No such legal provisions or general rules exist.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

    In terms of Article 843a CCP, the costs of disclosure pursuant to that provision are for the party requesting the disclosure of the documents.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

    Not applicable (see our answer to question 7).

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

    No (see our answer to question 7)

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    See our answer to question 20.

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

    a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

       The Netherlands data protection legislation is an implementation of the EU Privacy Directive 95/46/EC. The implementation legislation consists of the Act on the Protection of Personal Data of 6 July 2000 (*Wet bescherming persoonsgegevens*) (the "APPD") and the Exemption Decree of 7 May 2001 (*Vrijstellingsbesluit*) (the "Exemption Decree"). The purposes and guiding principles are in line with the EU privacy regime.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The terms "personal data" and "processing", are defined in article 1 of the APPD:

> "Personal data" means "any information relating to an identified or identifiable natural person".
>
> "Processing of personal data" means "any operation or any set of operations concerning personal data, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of data".

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

In order to be legitimate, the purposes for any processing should correspond to one of the legal bases for the processing of personal data described in the APPD, which include processing which is necessary (i) in order to comply with a *Dutch* legal obligation or (ii) to serve the *legitimate interest* of the data controller or a third party, provided that the privacy of the data subjects does not prevail. This ground entails a balancing of interests.

If personal data is further processed for a different (secondary) purpose than for which it was collected (*e.g.,* disclosure/production of documents in legal proceedings or regulatory enquiries), such secondary purpose should also correspond to one of the legal bases described in the APPD for which personal data is processed, and the primary and secondary purpose should be compatible. As a general rule: if processing is necessary for establishing, exercise or defence of a right in law, such processing will be allowed. Again, interests will have to be balanced, and the principles of subsidiarity and proportionality will have to be complied with. This entails that if documents to be disclosed contain personal data that are not relevant for the case at hand (like (mobile) phone numbers, health data), *such data will have to be redacted.*

If personal data is to be transferred to a country outside the European Economic Area ("EEA") that does not provide a so-called "adequate level of data protection," [230] stricter rules apply. A transfer is only permitted if one of the exemptions listed in the APPD applies, which include a transfer which is necessary for the establishment, exercise or defence of a right in law. This exemption only applies *in the context of legal proceedings* and is interpreted strictly. A subpoena from a foreign authority may in principle provide a basis for the transfer of (parts of) the personal data requested in such subpoena.

Additional restrictions apply to the processing of so-called *sensitive* personal data – such as one's race, religion, political preference, health, sexual preference, membership to a professional association, or criminal records. Such restrictions, however, do not apply if the processing of sensitive personal data is necessary for the establishment, exercise or defence of a right in law in the context of legal proceedings (please also see above).

---

[230] Countries providing such a level of protection are listed by the European Commission (*see* www. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm). Although the U.S. is not deemed to have an adequate level of protection, an exemption is made for U.S. companies that adhere to the so-called Safe Harbor principles (*see* www.http://www.export.gov/safeharbor/doc_safeharbor_index.asp).

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

There is no distinction in the Netherlands between civil and criminal proceedings in as far as it concerns data protection and privacy legislation, regulation or contracts.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Data subjects (individuals of whom data will be or are being processed) have several rights as to the processing of their personal data:

(i) Right to information

Pursuant to the AAPD, the data controller[231] must provide the data subject with the following information prior to obtaining the personal data, unless the data subject is already acquainted with this information: (i) the identity of the data controller; (ii) the purposes of the data processing; and (iii) other relevant information, such as the identity of recipients of the data, the nature of (the categories of) personal data processed, the right of the data subject to have access to his data and the right to request rectification of data. In the event of transfer of data to a country outside the EU that does not provide for an adequate level of protection of personal data, the data controller must inform the data subject of the fact that this is occurring and for what purposes, as well as the level of protection offered by the relevant country.

(ii) *Right of access*

Upon written request, the data controller must provide the data subject with a *full* and clear overview of the relevant personal data that are being processed, including a definition of the purposes of the processing, the categories of processed data and the (categories of) recipients, as well as the available information as to the origin of the data. According to the Dutch Supreme Court the data controller should provide *all* relevant information. A rough overview will not be sufficient. In principle the data controller should provide the data subject with *copies* of all relevant documents. However this does not entail an automatic right of the data subject to receive copies. The data controller may meet its obligations in another manner (under circumstances providing a summary and allowing inspection may be sufficient).

(iii) *Right of correction*

Data subjects may ask the data controller to correct, supplement, delete or block personal data relating to the relevant data subject in so far as such data are inaccurate, incomplete or irrelevant for the purposes of the processing, or are being processed in any other way that infringes a legal provision.

(iv) *Right to object*

Data subjects have a right to object to processing of their data on the basis of compelling grounds related to their particular situation.

[231] The "data controller" is the person/company/organisation that is responsible for determining the means and purposes of a given processing of personal data.

(v) *Other*

If a data subject is subjected to a decision which is based solely on automated processing of personal data, the data controller must provide information concerning the underlying logic of such automated decision.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

The APPD does not apply to the processing of personal data:

(i) in the course of a purely personal or household activity;

(ii) by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*);

(iii) for the purposes of implementing the police tasks defined in (Article 2 of) the Police Act 1993 (*Politiewet 1993*);

(iv) governed by or under the Municipal Database (Personal Records) Act (*Wet gemeentelijke basisadministratie persoonsgegevens*);

(v) for the purposes of implementing the Judicial Documentation Act (*Wet justitiële documentatie*);

(vi) for the purposes of implementing the Electoral Provisions Act (*Kieswet*), and

(vii) for exclusively journalistic, artistic or literary purposes; although certain provisions regarding the conditions for the lawful processing of personal data, the security of personal data, certain obligations of the data controller and the provision for liability for damages may still apply.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

There are no specific restrictions with respect to electronic discovery in the APPD. The general discovery regime and restrictions thereof have been dealt with elsewhere in this overview.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

Personal data may only be processed for specified and legitimate purposes (see above under (c)). In addition to the legal basis mentioned under (c), *unambiguous consent* of a data subject also constitutes a legal basis for processing of personal data. For the validity of unambiguous consent of employees, see our answer to question 20(k).

The Dutch Data Protection Authority ("Dutch DPA") (*College Bescherming Persoonsgegevens*) has issued rules of thumb for monitoring employees' use of email and internet. Pursuant to these rules monitoring should amongst others:

(i) initially take place in an automated way on the basis of keywords and/or the names of certain senders or recipients;

(ii) be initially restricted to subject headers (*i.e.,* will initially disregard the contents of correspondence);

(iii) disregard private correspondence (according to subject header (*e.g.,* correspondence with family));

(iv) disregard privileged information (*e.g.,* correspondence with company doctor, members of the works council);

(v) be restricted to the period of time relevant for the purposes of the investigation.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The data controller should notify the Dutch DPA of the processing of personal data, unless such processing is subject to an exemption. These exemptions are listed in the Exemption Decree. Failure to comply with the notification obligation is a violation of the Dutch DPA and can result in criminal fines. The Dutch DPA will publish the notification in a public register. Transparency of data processing is the main purpose of notification.

If personal data is to be transferred to a country outside the EEA which does not provide an adequate level of data protection, the Dutch DPA should be notified of the transfer. In addition, such data transfer may require, depending on the situation, that the data exporter and the data importer have entered into EU model contracts and the data exporter has obtained a data transfer permit from the Dutch Minister of Justice.

If the data controller wishes to perform an internal investigation into any irregularities of a criminal nature (also) on behalf of a third party (*e.g.,* a supervisory authority), a prior investigation of the Dutch DPA may be required.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

There are no *specific* procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations. For general considerations regarding litigation and regulatory investigations see above under (c). For obtaining information, see our answer to questions 20(f) and (j). In addition, the requirement of proportionality entails that personal data which is not strictly necessary for the purpose of the processing must be disregarded. This means that insofar as it is possible to anonymise information to be disclosed in legal proceedings or to be provided to a supervisory authority, this should be done.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

Unambiguous consent should be given *specifically* and *freely*. Because of the subordinate relationship between an employer and an employee, employee consent is generally not considered as given freely. Consent of an employee to process his or her personal data may therefore not be valid and may not constitute a legal basis for processing of personal data.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Evidence may be submitted in any form (including documents, witnesses and expert opinions).

It is also possible to rely on evidence obtained in another country through procedural measures unavailable in the Netherlands.

Council Regulation No. 1206/2001 of 28 May 2001 on Cooperation between the Courts of the Member States in the Taking of Evidence in Civil or Commercial Matters applies in regard of the EU member states. According to this Regulation, foreign courts must directly address their requests to the Dutch courts that have jurisdiction on the witness to be heard or on the person holding the requested document. Subsequently, the Dutch courts need to process the request within 30 days. The parties themselves and representatives of the requesting court have the right to be present at the hearing of the witness by the Dutch judge. A requesting court may also be authorised to directly proceed to the taking of evidence if the witness voluntarily cooperates and no coercive measures are required.

In the case Council Regulation 1206/2001 does not apply, The Hague Convention of 1970 on the taking of evidence (as implemented in the Netherlands in 1981) or another bilateral treaty may apply. The Netherlands has, in accordance with Article 23 of the Hague Convention, declared that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

See answer to question 21(a).

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

See answer to question 21(a).

Singapore

Benjamin Ang **- *Lead Editor***
Rajesh Sreenivasan **- *Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

Singapore's legal system is based on the English common law. Singapore's law is founded on the Constitution, legislation, subsidiary legislation and judge-made law.

The Constitution lays down the fundamental principles and basic framework for the three organs of state, namely, the Executive (President and the Cabinet), the Legislature (President and Parliament – enacts legislation) and the Judiciary.

The Law relating to document disclosure is based on the Rules of Court (see below).

Constitution and Jurisdiction

Under Article 93 of the Constitution of the Republic of Singapore, judicial power in Singapore is vested in the Supreme Court and in such subordinate courts as may be provided for by any written law for the time being in force. The Honourable the Chief Justice is the head of the Judiciary.

Singapore's Court Structure

The Supreme Court is made up of the Court of Appeal and the High Court, and hears both civil and criminal matters. The Supreme Court Bench consists of the Chief Justice, the Judges of Appeal, Judges and the Judicial Commissioners of the Supreme Court. The Supreme Court Registry is headed by the Registrar who is assisted by the Deputy Registrar, Senior Assistant Registrars and Assistant Registrars. Justices' Law Clerks, who work directly under the charge of the Chief Justice, assist the Judges and Judicial Commissioners by carrying out research on the law, particularly for appeals before the Court of Appeal.

The Court of Appeal

The Court of Appeal hears appeals against the decisions of High Court Judges in both civil and criminal matters. It became Singapore's final court of appeal on 8 April 1994, when appeals to the Judicial Committee of the Privy Council were abolished. The Chief Justice sits in the Court of Appeal together with the Judges of Appeal. A Judge of the High Court may, on the request of the Chief Justice, sit in the Court of Appeal. The Court of Appeal is presided over by the Chief Justice, and in his absence, a Judge of Appeal or a Judge of the High Court. The Court of Appeal is usually made up of three Judges. However, certain appeals, including those against interlocutory orders, may be heard by only two Judges. If necessary, the Court of Appeal may comprise five or any greater uneven number of Judges.

The High Court

The High Court consists of the Chief Justice and the Judges of the High Court. A Judge of Appeal may also sit in the High Court as a Judge. Proceedings in the High Court are heard before a single judge, unless otherwise provided by any written law. The High Court may also appoint one or more persons with expertise in the subject matter of the proceedings to assist the court. The High Court hears both criminal and civil cases as a court of first instance. The High Court also hears appeals from the decisions of District Courts and Magistrate's Courts in civil and criminal cases, and decides points of law reserved in special cases submitted by a District Court or a Magistrate's Court. In addition, the High Court has general supervisory and revisionary jurisdiction over all subordinate courts in any civil or criminal matter.

With a few limited exceptions, the High Court has the jurisdiction to hear and try any action where the defendant is served with a writ or other originating process in Singapore, or outside Singapore in the circumstances authorised by Rules of Court; or where the defendant submits to the jurisdiction of the High Court. Generally, except in probate matters, a civil case must be commenced in the High Court if the value of the claim exceeds $250,000.00. Probate matters are commenced in the High Court only if the value of the deceased's estate exceeds $3,000,000.00 or if the case involves the resealing of a foreign grant. In addition, ancillary matters in family proceedings involving assets of $1,500,000.00 or more are also heard in the High Court.

The following matters are also exclusively heard by the High Court:

- Admiralty matters;
- Company winding-up proceedings;
- Bankruptcy proceedings; and
- Applications for the admission of advocates and solicitors.

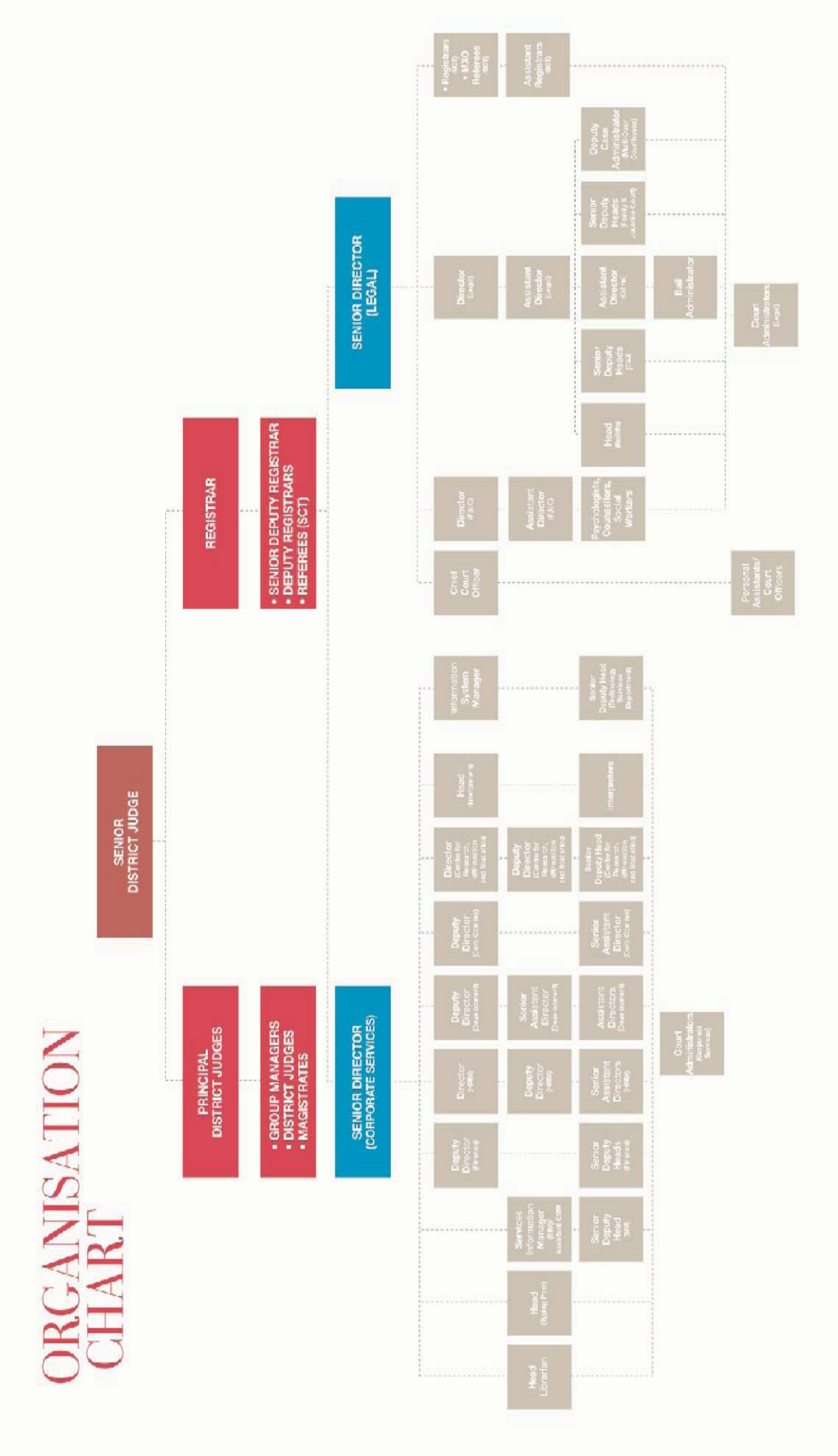
The High Court has jurisdiction to try all offences committed in Singapore and may also try offences committed outside Singapore in certain circumstances. In criminal cases, the High Court generally tries cases where the offences are punishable with death or imprisonment for a term which exceeds 10 years.

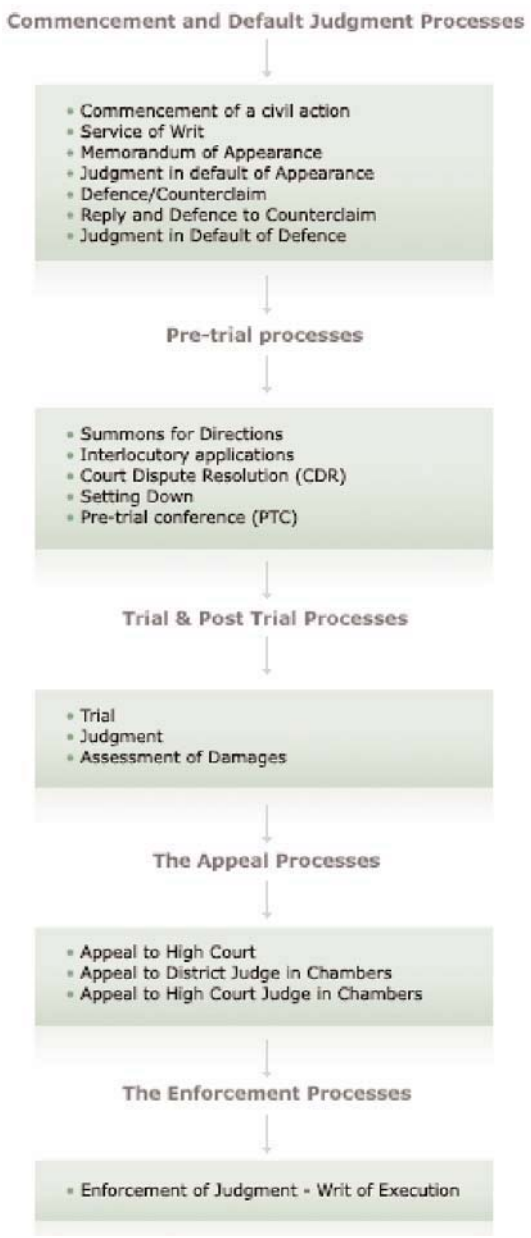
The Subordinate Courts

The Subordinate Courts comprise of:

- Family Justice
- Juvenile Justice
- Civil Justice
- Criminal Justice

The Subordinate Courts organization chart is attached on the next page.


ORGANISATION CHART
SENIOR DISTRICT JUDGE
PRINCIPAL DISTRICT JUDGES
• GROUP MANAGERS
• DISTRICT JUDGES
• MAGISTRATES
REGISTRAR
• SENIOR DEPUTY REGISTRAR
• DEPUTY REGISTRARS
• REFEREES (SCT)
SENIOR DIRECTOR (LEGAL)
SENIOR DIRECTOR (CORPORATE SERVICES)



2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

Pre-trial processes

Summons For Directions

Parties apply to court for directions pertaining to the filing and exchanging of affidavits, the number of witnesses a party may require, and the number of days a case may require are decided at this stage. Parties will also need to agree on specific evidence such as expert advice or photographs to be used in trial.

Interlocutory applications

During the pre-trial stages, both parties have to comply with the requirements set out in the Rules of Court, for example, those relating to giving further details of the facts of one's case, the gathering and exchange of documents to prove one's case (discovery) and the preparation and exchange of witness' statements (by way of affidavits of evidence-in-chief) which each party is relying on.

In the course of preparing the case for trial during the pre-trial stages, each party may file interlocutory application to the court in order to further the preparation of his case, *e.g.,* for discovery – through this process, the court can order that parties disclose to each other the documents in their possession, custody or power which are relevant to the matter in dispute between them.

Under Order 24 (Discovery and Inspection of Documents):

Order for discovery (O. 24, r. 1 Rules of Court)

1.—(1) Subject to this Rule and Rules 2 and 7, the Court may at any time order any party to a cause or matter (whether begun by writ, originating summons or otherwise) to give discovery by making and serving on any other party a list of the documents which are or have been in his possession, custody or power, and may at the same time or subsequently also order him to make and file an affidavit verifying such a list and to serve a copy thereof on the other party.

(2) The documents which a party to a cause or matter may be ordered to discover under paragraph (1) are as follows:

(a) the documents on which the party relies or will rely; and

(b) the documents which could —

(i) adversely affect his own case;

(ii) adversely affect another party's case; or

(iii) support another party's case.

(3) An order under this Rule may be limited to such documents or classes of documents only, or to only such of the matters in question in the cause or matter, as may be specified in the order.

Order for determination of issue, etc., before discovery (O. 24, r. 2 Rules of Court)

2.—(1) Where on an application for an order under Rule 1 it appears to the Court that any issue or question in the cause or matter should be determined before any discovery of documents is made by the parties, the Court may order that that issue or question be determined first.

(2) Where in an action begun by writ an order is made under this Rule for the determination of an issue or question, Order 25, Rules 2 to 7 shall, with the omission of so much of Rule 7(1) as requires parties to serve a notice specifying the orders and directions which they desire and with any other necessary modifications, apply as if the application on which the order was made were a summons for directions.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Discovery against other person (O. 24, r. 6 Rules of Court)

6.—(1) An application for an order for the discovery of documents before the commencement of proceedings shall be made by originating summons and the person against whom the order is sought shall be made defendant to the originating summons.

(2) An application after the commencement of proceedings for an order for the discovery of documents by a person who is not a party to the proceedings shall be made by summons, which must be served on that person personally and on every party to the proceedings.

(3) An originating summons under paragraph (1) or a summons under paragraph (2) shall be supported by an affidavit

…

(5) An order for the discovery of documents before the commencement of proceedings or for the discovery of documents by a person who is not a party to the proceedings may be made by the Court for the purpose of or with a view to identifying possible parties to any proceedings in such circumstances where the Court thinks it just to make such an order, and on such terms as it thinks just.

(6) An order for the discovery of documents may —

(a) be made conditional on the applicant's giving security for the costs of the person against whom it is made or on such other terms, if any, as the Court thinks just; and

(b) require the person against whom the order is made to make an affidavit stating whether the documents specified or described in the order are, or at any time have been, in his possession, custody or power and, if not then in his possession, custody or power, when he parted with them and what has become of them.

(7) No person shall be compelled by virtue of such an order to produce any document which he could not be compelled to produce —

(a) in the case of an originating summons under paragraph (1), if the subsequent proceedings had already been commenced; or

(b) in the case of a summons under paragraph (2), if he had been served with a subpoena to produce documents1 at the trial.

(8) For the purpose of Rules 10 and 11, an application for an order under this Rule shall be treated as a cause or matter between the applicant and the person against whom the order is sought.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

Singapore Courts would follow authorities from common law jurisdictions in respect of the preservation of documents for the purpose of civil proceedings, and when that obligation arises. I have also attached a useful Singapore Academy of Law Journal article *Recent Developments in Electronic Discovery: Discovering Electronic Documents and Discovering Documents Electronically*.

The solicitor's general obligation to preserve discoverable documents was recently summarized in the High Court decision in *Hong Leong Singapore Finance Ltd. v. United Overseas Bank Ltd.* by Sundaresh Menon, J.C. as requiring solicitors to take positive steps to ensure that their clients appreciate at an early stage of the litigation, promptly after the writ is issued if not sooner, not only the duty of discovery and its width but also the importance of not destroying documents which might possibly have to be disclosed.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

Failure to comply with requirement for discovery, etc. (O. 24, r. 16 Rules of Court)

16.—(1) If any party who is required by any Rule in this Order, or by any order made thereunder, to make discovery of documents or to produce any document for the purpose of inspection or any other purpose, fails to comply with any provision of the Rules in this Order, or with any order made thereunder, or both, as the case may be, then, without prejudice to Rule 11 (1), in the case of a failure to comply with any such provision, the Court may make such order as it thinks just including, in particular, an order that the action be dismissed or, as the case may be, an order that the defence be struck out and judgment be entered accordingly.

(2) If any party or person against whom an order for discovery or production of documents is made fails to comply with it, then, without prejudice to paragraph (1), he shall be liable to committal.

(3) Service on a party's solicitor of an order for discovery or production of documents made against that party shall be sufficient service to found an application for committal of the party

> disobeying the order, but the party may show in answer to the application that he had no notice or knowledge of the order.
>
> (4) A solicitor on whom such an order made against his client is served and who fails, without reasonable excuse, to give notice thereof to his client shall be liable to committal.
>
> (5) A party who is required by any Rule in this Order, or by any order made thereunder, to make discovery of documents or to produce any document for the purpose of inspection or any other purpose, but who fails to comply with any provision of that Rule or with that order, as the case may be, may not rely on those documents save with the leave of the Court.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

Costs of discovery/disclosure are treated as costs in the cause, *i.e.,* the eventual loser pay the eventual winner's costs.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

Singapore has no case law or specific rules relating to electronic disclosure, and it is likely to adopt some combination of the U.S., U.K. and Australian (Victoria) law. Some proposed amendments to the Rules of Court include amending O 25, r 3 to include a duty for parties to discuss and agree, at the Summons For Direction stage, issues that may foreseeably arise from the discovery of electronically stored documents and the possibility of providing discovery in electronic form.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

In July 1998, the Electronic Transactions Act (ETA) (Cap 88) was enacted to provide a legal foundation for electronic signatures and to give predictability and certainty to contracts formed electronically. The law addresses issues that arise in the context of electronic contracts and digital signatures. The Singapore ETA follows closely the UNCITRAL Model Law on Electronic Commerce, which sets the framework for electronic laws in many countries. The following provisions apply:

> **Legal recognition of electronic records**
>
> 6. —For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.
>
> **Requirement for writing**
>
> 7. —Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.

Retention of electronic records

9. —(1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; and

(d) the consent of the department or ministry of the Government, organ of State or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) (c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.

(4) Nothing in this section shall —

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; or

(b) preclude any department or ministry of the Government, organ of State or a statutory corporation from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department or ministry of the Government, organ of State or statutory corporation.

The Evidence Act (Cap 97) was also amended in 1997 to allow the use of electronic records as evidence in the courts. The following provision applies:

Rules for filing and receiving evidence and documents in court by using information technology

36A.—(1) The Rules Committee constituted under the Supreme Court of Judicature Act (Cap. 322) may make rules to provide for the filing, receiving and recording of evidence and documents in court by the use of information technology in such form, manner or method as may be prescribed.

[8/96]

(2) Without prejudice to the generality of subsection (1), such rules may —

(a) modify such provisions of this Act as may be necessary for the purpose of facilitating the use of electronic filing of documents in court;

(b) provide for the burden of proof and rebuttable presumptions in relation to the identity and authority of the person sending or filing the evidence or documents by the use of information technology; and

(c) provide for the authentication of evidence and documents filed or received by the use of information technology.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

There are no specific legal provisions or rules in place, but some proposed amendments to the Rules of Court include amending O 25, r 3 to include a duty for parties to discuss and agree, at the Summons For Direction stage, issues which may foreseeably arise from the discovery of electronically stored documents and the possibility of providing discovery in electronic form.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

The Rules of Court (see above) as interpreted by the case of *Hong Leong Singapore Finance Ltd. v. United Overseas Bank Ltd.* indicates the requirement to preserve documents in general. The Evidence Act and Section 9 of the Electronic Transactions Act (see above) would extend that requirement to include electronic documents.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

The Rules of Court (see above) specify the scope of a party's obligation to search for, disclose and produce documents in general. The Evidence Act and Section 9 of the Electronic Transactions Act (see above) would extend that requirement to include electronic documents.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

There are none in place.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

There are none in place. However, the Electronic Filing System Review Committee convened by the Chief Justice developed an Electronic Litigation Roadmap in 2005:

> The Electronic Litigation Roadmap charts a course for the deployment of technology in the litigation process in Singapore. The end goal is to facilitate the disposal of cases and thereby enhance access to justice.
>
> …
>
> 2.4 The aim of this Roadmap is to provide general guidelines and direction to bind future implementing committees carrying out these recommendations. Further, it is envisaged that the

different stakeholders from both the private and public sectors may participate in different components of the ELS.

Order 63A of the Singapore Rules of Court ("O63A")

While not strictly relevant to the issue of how electronic documents must be presented to the other party as part of E-Discovery or E-Disclosure, O63A was an inclusion to the Singapore Rules of Court as part of the move toward greater use of information technology in the Court process in Singapore, with a view to improving efficiency in the administration of justice in Singapore.

O63A is relevant in so far as it lays down the rules that parties to litigation must adhere to in presenting digital versions of court documents filed electronically through the Electronic Filing Services' "File-n-Serve" feature.[232]

O63A comprises 18 rules on the issue of electronic filing and deemed service of electronically filed court documents. The range of issues O63A deals with include: signature requirements in relation to electronically filed documents,[233] deemed date of filing,[234] deemed service of electronically filed documents (save for documents required to be served personally),[235] and the presumptions created upon successful electronic filing of documents.[236]

The Singapore courts have interpreted O63A in the recent past,[237] and a significant pronouncement that they have made is that documents properly filed electronically are, pursuant to O63A, r.12, deemed served on the other party or parties to the relevant court action once the documents have been received by the electronic filing registry,[238] as opposed to when the electronically filed documents are actually retrieved by the intended recipient(s).[239]

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

The legal standards are the same as those required for hardcopy documentary evidence.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

Restriction on use of privileged document, inspection of which has been inadvertently allowed (O. 24, r. 19 Rules of Court)

19. Where a party inadvertently allows a privileged document to be inspected, the party who inspected it may use it or its contents only if the leave of the Court to do so is first obtained.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

Costs of discovery/disclosure are treated as costs in the cause, *i.e.,* the eventual loser pay the eventual winner's costs.

---

[232] For an overview of the EFS system in use in Singapore, *see* http://info.efs.com.sg/default.htm (last visited 20 July 2008).
[233] *See* O63A, r.9.
[234] *See* O63A, r.10.
[235] *See* O63A, r.12.
[236] *See* O63A, r.16.
[237] *See Firstlink Energy Pte Ltd. v. Creanovate Pte Ltd.* [2006] S.G.H.C. 19.
[238] CrimsonLogic Pte Ltd. in Singapore's case.
[239] *See Firstlink Energy Pte Ltd. v. Creanovate Pte Ltd.* [2006] S.G.H.C. 19, per Yeong Zee Kin AR at paragraphs 10 – 12 inclusive.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

The author was a director in the Singapore offices of two multi-national professional services firms. Both firms implemented information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes. There is also anecdotal evidence of other multi-national companies applying such policies and procedures to their Singapore officers. It is unclear whether this is widespread among small or medium sized local businesses.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

There is a growing awareness of such technologies, and a number of vendors are offering such services in the Singapore market.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

There are no privacy rules in Singapore. The one limitation to discovery is as follows:

> **Document disclosure of which would be injurious to public interest: Saving (O. 24, r. 15 Rules of Court)**
>
> 15. Rules 1 to 14 shall be without prejudice to any rule of law which authorizes or requires the withholding of any document on the ground that the disclosure of it would be injurious to the public interest.

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

The Singapore Constitution is based on the British system and does not contain any explicit right to privacy.[240] The High Court has ruled that personal information may be protected from disclosure under a duty of confidences.

There is no general data protection or privacy law in Singapore. The government uses surveillance to promote law and order[241] – there are cameras on all highways and many street corners. To quote the former Prime Minister and founder of modern Singapore, Lee Kwan Yew:

> I am often accused of interfering in the private lives of citizens. Yet, if I did not, had I not done that, we wouldn't be here today. And I say without the slightest remorse, that we wouldn't be here, we would not have made economic progress, if we had not intervened on very personal matters – who your neighbor is, how you live, the noise you make, how you spit, or what language you use. We decide what is right, never mind what the people think. That's another problem.[242]

[240] *X v. CDE* 1992 2 S.L.R. 996.
[241] Christophen Tremewan, The Political Economy of Social Control in Singapore (St. Martin's Press, 1994).
[242] "Lee Kwan Yew's Speech at National Day Rally," The Straits Times, April 20, 1987, cited in Christophen Tremewan, *id.*

In 2005-2006, the government set up an inter-ministerial sub-committee to look at laws to protect the privacy of individuals, under the National Infocomm Security Committee. Sixteen government agencies, including the Finance and Trade and Industry Ministries, sit on this sub-committee, which will recommend legislation as well.

The Public sector has strict laws protecting the confidentiality of data held by the government and statutory boards:

- Official Secrets Act
- Statistics Act
- Central Provident Fund Act
- Electronic Transactions Act

The Private sector relies on industry codes of practice, and sector-specific laws.

- Computer Misuse Act – creates a criminal offence to access without authority.
- Telecommunications Act and Telecom Competition Code – creates a criminal offence to access without authority.
- Banking Act.

For the rest, there is the Common law protection of the Law of Confidence/Confidential Information – the party alleging breach of confidence must show:

- Information has quality of confidence,
- Information is imparted within a relationship of confidentiality, and
- Unauthorised use and disclosure.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The legal definition can be found in different statutes:

Under the Electronic Transactions Act, "information" includes data, text, images, sound, codes, computer programs, software and databases.

The most comprehensive can be found in Section 47 of the Banking Act:

Banking secrecy

47.—(1) Customer information shall not, in any way, be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided in this Act.

(2) A bank in Singapore or any of its officers may, for such purpose as may be specified in the first column of the Third Schedule, disclose customer information to such persons or class of persons as may be specified in the second column of that Schedule, and in compliance with such conditions as may be specified in the third column of that Schedule.

(3) Where customer information is likely to be disclosed in any proceedings referred to in item 3 or 4 of Part I of the Third Schedule, the court may, either of its own motion,

or on the application of any party to the proceedings or the customer to which the customer information relates —

(a) direct that the proceedings be held in camera; and

(b) make such further orders as it may consider necessary to ensure the confidentiality of the customer information.

(4) Where an order has been made by a court under subsection (3), any person who, contrary to such an order, publishes any information that is likely to lead to the identification of any party to the proceedings shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $125,000.

(5) Any person (including, where the person is a body corporate, an officer of the body corporate) who receives customer information referred to in Part II of the Third Schedule shall not, at any time, disclose the customer information or any part thereof to any other person, except as authorised under that Schedule or if required to do so by an order of court.

(6) Any person who contravenes subsection (1) or (5) shall be guilty of an offence and shall be liable on conviction —

(a) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or

(b) in any other case, to a fine not exceeding $250,000.

. . .

(9) Where, in the course of an inspection under section 43 or an investigation under section 44 or the carrying out of the Authority's function of supervising the financial condition of any bank, the Authority incidentally obtains customer information and such information is not necessary for the supervision or regulation of the bank by the Authority, then, such information shall be treated as secret by the Authority.

c. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

Electronic Transactions Act – Production of documents, data, etc. Section 55.

The Controller or an authorised officer shall, for the purposes of the execution of this Act, have power to do all or any of the following: (a) require the production of records, accounts, data and documents kept by a licensed certification authority and to inspect, examine and copy any of them; (b) require the production of any identification document from any person in relation to any offence under this Act or any regulations made thereunder; (c) make such inquiry as may be necessary to ascertain whether the provisions of this Act or any regulations made thereunder have been complied with.

The National Internet Advisory Committee published its e-commerce code in Sept, 1998, as a voluntary scheme establishing standards of behaviour for ISPs and Internet content providers. The Code is administered by CaseTrust (a Compliance Authority or self-regulatory certification body)

that grants the use of a Privacy Code Compliance SymbolÅ to companies that comply with the Code. The objectives include:

- To provide minimum standards for the use and management of personal information of Internet users.
- To protect the confidentiality of private communications.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

Yes.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

To the extent that there is protection, natural and legal persons have rights.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

Not clear.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

Please see above for restrictions on discovery.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

Not clear.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

This does not apply.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

The discovery process is unchanged.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

This is not required and not applicable.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Singapore is a party to the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters.[243]

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

Singapore is one of several countries that have enacted blocking statutes. In response, "the United States has entered into various consular treaties and consular conventions to facilitate the taking of discovery in foreign countries" by U.S. litigants. The author has no published information on enforcement.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The author has no published information on enforcement.

[243] Hague Evidence Convention codifies the taking of depositions on notice and commission before consuls and court appointed commissioners, providing minimum standards with which contracting states agree to comply. The Convention's primary purpose is to reconcile different, often conflictive, discovery procedures in civil and common law countries. The Convention also streamlines procedures for compulsion of evidence, utilizing a form "letter of request" which can be sent directly by the court in the U.S. to a foreign central authority, eliminating the cumbersome "diplomatic channel."

Spain

Miguel Torres - ***Lead Editor***
Christian Gual - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

Spain is a civil law country. The Spanish legal system is a typical civil law system in which the main manifestations of the law are codified. Hence, there is a main branch of the law – the civil law – from which the whole private law has derived, in particular the Commercial law. Article 1.1 of the Civil Code states that "The sources of the Spanish legal system are the law, custom and the general principles of jurisprudence."

Article 117.1 of the Spanish Constitution states that the judges are independent, undetachable, liable and subject only to the law. Paragraph 3 of same Article, states that the jurisdiction in all kind of proceedings, rendering decision and enforcing the same correspond exclusively to the Courts determined by the laws,[244] in accordance with the competence and jurisdiction and procedural rules envisaged in the law.

The Spanish judicial system is organised pursuant to the provisions of the Organic Law of the Judicial Power (hereinafter referred to as OLJP). The Courts are organised in different jurisdictional orders upon the matters: Civil (including commercial matters), Criminal, Administrative, Labour and Social and, finally, Military. Articles 22 to 25 OLPJ rule the matters that fall within each of the orders, while the international Treaties and Conventions to which Spain is a party should also be respected by the Courts while exercising its duties.

Disregarding the Constitutional Court, which is not deemed as a jurisdictional body, as it only deals with constitutional matters, the ordinary judicial system is organised as follows:

(a) Supreme Court: it is the highest court, formed by five chambers: I. Civil (including commercial matters); II. Criminal; III. Administrative; IV. Labour and Social and, V. Military. Technically speaking, only a repeated decision of the Supreme Court can be considered "*jurisprudencia*"[245] (which would be the approximate translation for "case law").

(b) High Courts of Justice (Tribunales Superiores de Justicia): there are 17, one in each Autonomous Community. Each of them is formed by three Chambers: I. Civil and Criminal, II. Administrative, III. Labour and Social. Moreover a Chamber may have sections and/or be located in different places. It should be noted that in those territories that have special civil rules (basically, Cataluña, Aragón, Navarra and Baleares), different from the Civil Code, the Civil Chambers take the role of the Supreme Court in those cases that the lawsuit only deals with the construction of such local rules.

(c) Courts of Appeal (*Audiencias Provinciales*): There are 50, one in each province (they may have several chambers or even these be located in different cities of the province). They deal with appeals on Civil

[244] This must be understood without prejudice to the possibility to conduct arbitration proceedings if the parties agree to do so and the subject-matter of the dispute is at their free disposal. At least from a practical standpoint, both arbitration and (to a lesser extent) ADR systems, form part of the Spanish dispute resolution panorama.
[245] Not the jurisprudence (*principios generales del Derecho*) referred to in the first paragraph quote of article 1.1 of the Civil Code.

and Criminal matters, while in the latter case they take the role sometimes of First Instance Court, when the crimes involved are especially serious.

(d) First Instance Courts: although this name is given to Civil Courts, first instance ones are also Labour, Criminal and Administrative. Its number depends on the population of each place where they are located. They have jurisdiction over the so called "*partidos judiciales,*" which are smaller areas than a province. For instance, the city of Madrid has over 75 Civil Courts while a small place has normally two or three, covering not only such town but also other located within the same territory.

(e) Courts of Peace: there is one in each town where there is no first instance Civil Court. They are not served by judges and their main duty is to decide on discussions about very small claims (€90), unless due to the nature of the matter it would correspond to a first instance Civil Court.

A brief overview of how civil litigation is conducted in practice.

On January 5, 2001 a new Civil Proceeding Act, 1/2000, (hereinafter referred to as "CPA") came into force. The CPA states two types of declaratory proceedings, ordinary and verbal, discovery rules, and four types of special proceedings, as well a cautionary measures and the enforcement rules. The most important feature is that the first instance proceedings are mainly oral.

The ordinary proceeding is divided in four basic stages: (i) file of statements of claim and defense and counterclaim, if any; (ii) case management hearing. This stage has several purposes, first the judge tries that the parties settle the matter. If it is not possible, the Court will deal with any procedural circumstance which may prevent to render a decision on the merits of the case and, if there is none, the parties are entitled to propose the evidence that they want to produce and discuss about the correctness of the documents already produced; (iii) the trial, where the evidence is produced (interrogatory of the parties, witnesses, expert reports, videos, electronic evidence, etc.); and (iv) the Judgment.

The verbal proceeding is shorter: the claimant files the statement and the Court calls the defendant to the hearing, in which the defendant answer orally the claim and the parties produce all evidence it deem convenient and report the Court about it's conclusions. After this, the Court renders its judgment. The rules for this proceeding are also applicable for certain hearings such as interim measures.

The duration depends basically on each Court but an average for the first instance, provided that no special evidence is taken, for instance rogatory commissions, could be around four to six months for the verbal proceeding and nine to twelve months for the ordinary proceeding.

Remedies. Article 448 CPA expressly acknowledges the right of the parties to appeal any judicial resolution that prejudices parties' rights, save for those specifically excluded of direct appeal.

Further to interlocutory resolutions, which may be appealed before the same instance, First Instance Judgments or Orders (*Autos*) may be appealed before the *Audiencia Provincial* (Court of Appeal). Judgments or Orders rendered by these Courts may be challenged through two different ways: the traditional remedy of cassation before the Supreme Court, which is limited to the breach of material statute or regulations, provided the amount of the claim exceeds €150,253, or when the matter would have cassational interest,[246] and a new remedy, called "extraordinary remedy for procedural breach," which will be handled before the Civil Chamber of the Tribunal Superior de Justicia of each Autonomous Community. This remedy will only be admitted if the party

[246] The CPA sets a double criteria to establish what proceeding (*i.e.,* ordinary or verbal) must be followed: (i) subject matter of the dispute (both Articles 249 and 250 of the CPA set the corresponding list) and (ii) amount of the claim. This is now relevant because the Supreme Court has adopted the following criteria: if the proceeding has been determined on the basis of the subject-matter, then cassational interest should always be justified (*i.e.,* a mere reference to the amount of the claim exceeding €150,253 will not be enough).

has objected the alleged procedural breach, as the case may be, before the First Instance Court or the Court of Appeal, once such breach occurred in the opinion of the party.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

In general terms, it could be said that there is no obligation to disclose. Obviously, when a party raises an allegation it must prove the facts upon which the allegation is based, but it will keep control of the specific means of evidence it wants to use and, particularly concerning documents, the specific documents it wants to show the Court. This is, as of today,[247] a basic rule of Spanish civil litigation. Another strong principle is "preclusión," which, one might say, is a sort of statute of limitation specially related to the judicial proceedings: if one should have said or done something at a particular stage of the proceedings, it will not be allowed to say it or do it at a subsequent stage.

Now, the sum of those two basic ideas or principles explain the following regulation:

Article 265 CPA states that certain documents should be filed with the claim. CPA divides documents in two types: procedural and material ones. The former should be attached to the statement of claim in any event (power of attorney, evidence of capacity to be party and, if necessary, those showing the value of the litigious thing) while the latter should only be attached in certain cases as a condition precedent for the claim to be admitted. In any event those documents or evidence on which the claimant bases his rights on the merits must be attached to the statement of claim. The defendant has the same burden about the documents related to his basic defenses.

Therefore, the parties should disclose their main documentary evidence (including electronic evidence) at the beginning of the process. This rule has however some exceptions (Article 267 CPA), as follows: (i) documents dated after the date in which the initial statements of the parties were filed; (ii) documents dated before said date or before the preliminary hearing, provided that the party justifies that it ignored their existence. Needless to say, this brings an additional burden to that party with the risk that the document may be rejected if the judge does not believe the ignorance about the existence of the document; and (iii) where it is not possible for the party to obtain the relevant documents without fault on his part. In practice, lawyers use to refer the court to the records of third parties, applying later on for these documents to be produced by such third parties.

The claimant has the additional right to be exercised in the case management hearing, in which he may file additional documents in response to the pleadings of the defendant (Article 265.3 CPA). The parties may also do so as a consequence of new facts or elements related to the proceeding under certain limited circumstances (Article 426.5 CPA). In practice, this means that the plaintiff may produce additional documents after having had a chance to review the defense of the other party while for the defendant it is more difficult, as he should bring documents in anticipation of possible additional pleadings of the plaintiff at the preliminary hearing.

Finally, under certain circumstances, mainly within the case management hearing and after the disputed facts have been reviewed, the Court can suggest to the parties that a particular allegation risks not being adequately proved with the evidences they have proposed. This is very unusual in practice.

[247] There is an increasing number of provisions that, when seen as a whole, seem to be willing to transform the proceedings into a more inquisitorial one, a more investigation oriented proceeding, to put it in plain words. These are, nevertheless, still exceptional provisions strictly related to some particular IP litigation disputes.

Pursuant to Article 299.1 CPA, evidence means are: (i) Parties interrogatory; (ii) public documents; (iii) private documents; (iv) experts' reports; (v) judicial examination; (vi) witnesses. CPA has expressly included as evidence means for reproducing words, image and sound, as well as instruments for the storage and retrieval of data, words, figures and mathematical operations carried out with accounting purposes or other relevant for the proceedings (Articles 299.2 and 382 CPA). Strictly speaking, these are not considered documents, although the Preamble of the CPA states that they should be considered analogous to documents. The assimilation to this type of evidence to documents has been expanded in other laws, namely the Act 34/2002 of Services of the Information Society and Electronic Commerce (ASISEC) and the Act 59/2003 of Electronic Signature (AES).

In Spain and for procedural purposes, documents are classified as "public" and "private." The former are listed by the law (*e.g.,* documents executed by a Notary Public, a register certification, administrative documents) and per se carry a certain evidentiary weight which in principle cannot be disputed (they prove conclusively the act that they are documenting, the date of execution and the identity of the signatories or other parties that have participated in such act). For instance, a notarised contract will give better evidence that a simple contract just signed by the parties, as for instance the parties are prevented to challenge that they are parties to said notarised contract. A foreign public document duly legalised will be also considered a public document for procedural and evidence purposes (for instance, a foreign certification of birth). On the other side, private documents are all those that are not public (Article 324 CPA).

If the document is considered untrue, incomplete or even false and, therefore, challenged in the case management hearing, the party that produced it may request the Court to take expert evidence on the document or any other evidence that could lead to establish the authenticity of the document. If it is established that the private document is correct and true or if it has not been challenged, Article 326 CPA states the private document will have the same evidentiary weight as a public document.

There is no possibility under the Spanish civil procedure rules for "fishing expeditions" as in the U.S., although there is an obligation of disclosure between the litigants. Article 328 CPA requires the parties to disclose the documents or evidence requested by the other and admitted by the Court. This petition should always refer to a particular document and should be made in the case management hearing. The document, however, should be related to the subject matter of the proceeding. When applying for disclosure, the party is obliged to attach a copy of the document or, if not available, to identify as far as possible the contents of the document or documents. Once the documents are produced, it would be possible to discuss if the information disclosed is complete or not. However, the possibilities of receiving unknown documents are certainly scarce as a consequence of the duty of identification. Generally speaking, the Courts are rather reluctant to grant wide petitions, unless in certain claims such as unfair competition, there is a reversal of the burden of the proof for the advantage of the claimant.[248]

In Spain, the party refusing to comply with an order of disclosure of documents may be subject to possible criminal penalties for contempt of court. In addition the judge has two courses of action: (i) to accept, taking into account the remaining evidence gathered, the copy filed by the proposing party or the party's version of the contents of the documents (adverse inferences) or (ii) to request once again the party to produce the document, provided that the features of the document make it necessary to see it and taking into consideration the other evidence produced by the parties and the position and allegations of the party that proposed such evidence (Article 329 CPA). Finally, according to Article 217 CPA, which deals with the burden of the proof, the Court shall consider to render judgment, the availability of the evidence for the parties and the easiness to produce it. This provision, without releasing of the burden of the proof, implies a more flexible stance and leads sometimes to accept a certain fact when the party that would be able to prove the contrary, does not take any

[248] In our opinion, the reversal of the burden of the proof does not necessarily entail a widest approach to the disclosure of documents and, for the same reason, does not automatically mean a widest obligation to disclose. It will still be the party bearing the burden who will decide what and to what extent it files a particular document with the Court.

activity relying only in the burden of the other. For instance, the Court of Appeal of Madrid decision of 11 May 2005 (AC 2005/967) accepted that a shareholder attend the general meeting even without direct evidence as the company did not provide the list of attendees, which is a legal duty and could have easily proved if the shareholder attended or not.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

As a general rule, Article 330 CPA sets forth that third parties may only be obliged to disclose documents when requested by any of the parties and the court would understand that the knowledge of the document may be essential for adjudicating the matter. In this event, the court would summon the third party to know whether it has any objection to disclose the evidence requested. The third party has the option to appear personally to show the documents and let the court make copies or request that a court official appears and makes the copy without taking the document away from the records. However, in practice, third parties use to send copies of the documents requested by post or a statement informing that they do not have the document. Pursuant to Article 332 CPA, governmental agencies or corporations always have the duty to disclose the requested information, save that it would be classified as confidential or secret, in which case it should inform the court in writing about the reasons for non-disclosure.

The CPA differentiates between preliminary evidentiary enquiries, a sort of pre-trial discovery (Articles 256 et seq. CPA) and advanced discovery including conservation of evidence (Articles 293 *et seq.* CPA).

Preliminary evidentiary enquiries

It is allowed for preparing the lawsuit by making available to the claimant certain documents, namely and strictly limited to wills, corporate documents and accounting (only for shareholders or partners), insurance policies, matters related to patents or trade marks or facts related to unfair competition. In addition to these cases which specifically involve documents, testimony may be required over facts related to capacity, representation or legal standing for being sued or to seek disclosure of documents proving that capacity, representation or legal standing. There are other instances in which pre-trial discovery could be sought but would not be relevant for this paper. If the party required to exhibit the documents would refuse without fair cause to deliver them, the court may order the entrance in the place where the documents are supposed to be, taking the documents and depositing them in the court at the disposal of the party (Article 261 CPA).

The court will assess its jurisdiction on its own motion and, if acceptable, it may request security to the applicant in order to cover possible damages. This bond shall be returned if no damages are caused and provided that the lawsuit starts within 30 days after receiving the documents or information requested.

The court will serve the requested party with the application and this party may oppose, in which case the court will summon the parties to a hearing. If the court finally accepts the application, there is no appeal while if rejected, the applicant may appeal to the upper court.

Advanced discovery

This is intended to avoid the loss of evidence and may be requested before starting litigation or while it is conducted, obviously prior to the stage of submitting evidence. The applicant must prove there is a sound risk ("founded fear" is the legal expression) that the evidence could not be produced at the appropriate stage.

The competent court is the one that would deal with the main proceeding if it has not been initiated yet. Evidence should be proposed in accordance with the general rules and, if accepted, the court shall take the

relevant steps including service to the parties concerned who may plead whatever they may deem convenient or even oppose the taking of evidence. Evidence so taken would not be valid, if the plaintiff does not file the statement of claim within two months from the date in which the evidence was produced.

Conservation of evidence

Before starting a proceeding or while it is pending, any party may request the court to take the necessary steps in order to avoid destruction of evidence that can be material for the lawsuit. The court can provide for a wide variety of measures leading to preserve things or situations or the means to prove such things and situations, and can order the parties to refrain from taking certain action, or order them to take certain action advising that it may proceed against them for contempt of court. The court should ensure that the following conditions are complied with:

(i) Evidence should be possible, adequate and useful when proposed;

(ii) Proof of reasons given;

(iii) Availability of the evidence without causing serious inconveniences to the other party or to third parties.

Finally, the court may require security to the applicant before taking the relevant steps or accept a bond from the requested party to compensate any possible damages that may derive from the lack of production of the requested evidence.

As can be seen, there is a fair degree of evidentiary activity available prior to the actual filing of the claim in court. Yet Spain radically banned pre-trial discovery under Article 23 of The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial matters of 18 March 1970.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

There are no obligations to preserve documents for the purpose of civil litigation as such. However, Article 30 of the Code of Commerce states the obligations for entrepreneurs to conserve correspondence, corporate and commercial documents concerning the business for at least six years. Therefore, a party may request from the other to disclose documents falling within those described in the assumption that they should exist. This notwithstanding, there are some exceptions. For instance, Royal Decree 629/1993 obliges to keep a register of orders related to stock sales or purchases, which could be of signed paper orders, record tapes or electronic storage. The Royal Decree was developed by the CNMV (Spanish Securities regulatory authority), stating the record or orders should be kept at least three years since the receipt of the order or the oral orders should be recorded for at least three months, although if there is any claim, the file should be kept until the dispute is resolved.

Generally speaking, Spanish law does not foresee that a direct request would oblige a party to preserve documents. Conservation would only be admitted through the judicial proceeding stated above. However, if a party is requested to preserve documents, the Court may balance against that party the rules about the burden of the proof if certain documents were destroyed simply because the legal deadline for conservation elapsed, disregarding the petition of the other party.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

   The CPA does not foresee any penalty as such. However, further to contempt of court (a criminal offence, however), pursuant to Article 329.1 CPA in the event of failure of disclosure without justification, considering the evidence which is available in the case, the Court is entitled to give evidentiary value to the simple copy filed by moving party or to the version of the content of said document as alleged by said party. Nonetheless, the Court may also order the production of such evidence. The consequences of the refusal are therefore prejudicial to the party refusing to disclose or alleging that the documents were lost. There could be administrative fines if the preservation time is not met.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

   Article 394 CPA states that the losing party will bear the costs, unless the case would be factually or legally doubtful in the opinion of the Court. If the legal expenses are awarded, they include fees of the lawyers and experts and witnesses costs but the law does not mention other costs.

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

   The absence of a general obligation to disclose (see introductory explanation to question 2) explains that there are no specific rules regarding e-discovery or e-disclosure.

   As to electronic evidence in general, to the best of our knowledge, there are few judicial decisions and mostly are previous to the CPA in force or have been issued by labour Courts (in the answer to question 19 there is a reference to a recent decision by the labour Chamber of the Supreme Court). The decisions based on the former CPA used to admit electronic evidence at large although as the CPA in force contains specific provisions for this, the matter is no longer controversial.

   Secondly and regarding specific rules developed, as above mentioned, further to the traditional evidence means, the CPA has expressly included as evidence means for reproducing words, image and sound, as well as instruments for the storage and retrieval of data, words, figures and mathematical operations carried out with accounting purposes or others relevant for the proceedings (Articles 299.2 and 384 CPA). In addition, the CPA admits any kind of evidence mean through which certainty about the facts discussed may be obtained. This final provision would allow for instance the view of a web-site during the trial.

   Testimonies throughout Spain or abroad may be taken through videoconference if the court so agrees, pursuant to Article 229.3 of the Judiciary Power Organic Act.

   In addition, both ASISEC and AES have included provisions for electronic evidence in connection with the matters regulated therein.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   Pursuant to Article 24 ASISEC, the evidence of the execution of an electronic contract and of the obligations arising there from will be governed by the general rules and those about electronic signature (AES), clarifying that the electronic support of a contract will be admissible as electronic evidence. This Act allows agreeing that

the consent statements contained in emails exchanged by the parties may be deposited with a third party, who does not need to be a notary public. It is clear that this possibility will ease the procedural position of the parties in the event of a dispute.

AES defines in Article 3.1 the electronic signature as the group of data in electronic form, together or associated with other data, which may be used to identify the signatory. The advanced electronic signature (Article 3.2) is that electronic signature that allows identifying the signatory and detecting any subsequent amendment in the signed data. It is linked to the signatory and the data to which it refers in a unique way and it must be created by means under the exclusive control of that person. Finally, recognized electronic signature (Article 3.3) is based in a recognized certificate and generated through a safe tool for creation of signatures.

In connection with the production of electronic documents, Article 3.8 AES states that media containing electronic data shall be admitted as documentary evidence. In those events that an electronic signature may be challenged, this provision states how the authenticity of the signature may be acknowledged. If the challenged signature is a recognized electronic signature, the Court will order to check that all the legal requirements for this type of signature were met. If an advanced electronic signature is challenged, then AES refers to Article 326.2 of the CPA, which states the possibility of an expert examination of the signature or any other evidence which may be useful to establish the certainty of the challenged signature or document.

Article 3.5 AES defines electronic document as any information in electronic form that is stored in a specific format and that can be separately identified and processed. Article 3.6 AES specifies that the electronic document may be (a) a public document, if electronically signed by a public officer able to give public faith; (b) documents issued and electronically signed by civil servants in the exercise of their public service and (c) private documents.

For jurisdictional purposes, Article 23 of the Council Regulation (EC) 44/2001 OF December 2000 on jurisdiction and recognition and enforcement of judgments in civil and commercial matters establishes the conditions for the valid prorogation of jurisdiction. Specifically, paragraph 2 sets forth that "any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing.'"

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

In the Spanish civil proceeding, no meeting is legally foreseen as such.[249] The only similarity would be the case management hearing, which is conducted before the Court. At that stage, the parties propose the Court the evidence and it is the Court who orders the exchange of documents, either electronic or not. A litigant is only obliged to disclose if ordered by the Court when, after the proposal, it considers such evidence useful for the case. Under certain circumstances, a party may be obliged to disclose documents in pre-trial proceedings.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

As above mentioned, there is a general obligation for preservation of business documents pursuant to Article 30 of the Code of Commerce, which may vary for certain type of business as above mentioned. In the absence of further clarification and considering that other procedural provisions give equal treatment to electronic documents, it should be understood that this preservation duty shall comprise electronic documents related to the business, including emails. However, this does not mean that any and all emails would be related to the business.

[249] These types of meetings are unusual in normal Spanish judicial civil litigation. Since every single step is legally regulated (terms to file allegations, number of hearings, etc.), there has never been the need to hold them. We only began to get used to them and to what we could call a private design of the procedural steps due to the increasing number of arbitrations.

Specifically regarding electronic documents, Article 25.1 ASESIC obliges the third party appointed by the contracting parties to conserve documents, to keep them for all the time agreed by the parties but in no event less than five years.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

As mentioned above, Spanish procedural law does not allow "fishing expeditions." However, nothing prevents to file a complete drive disk as evidence or request the examination of other information stored in servers or computers, with the limits of Article 328 and 329 CPA, as above explained. This notwithstanding, considering that the evidence should be relevant and useful for the proceeding, it is likely that the judge may impose restrictions about the search and the production of documents.

In addition, as also explained above, it would be possible to file a motion for conservation of evidence, pursuant to Articles 297 and 298 CPA.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

A party is obliged to produce the documents requested and therefore, no "search" is admissible. However, if a party considers that certain documents have not been disclosed with the extent determined by the Court at the case management hearing, even if they was an order to produce them, it will be possible to request the Court to order the production thereof, through the exceptional "*diligencias finales*." These are available when after the trial, accepted evidence has not been produced for reasons beyond the moving party.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

The CPA does not provide any special form. Paper or electronic format will be admissible but if a party requests electronic format and the Court accepts it, the requested party shall comply with such order. It is worth to mention that the electronic format shall probably include more information about the document than a mere printed copy. If the document is not challenged, it may not be necessary to produce the electronic version and a printed copy may be enough. However, considering the production constraints, it seems advisable to produce the most information with the respective statements of claim or defense.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

As we mentioned earlier, and assuming that the plaintiff has not applied for conservation in advance (Article 297 CPA), the parties are obliged to produce (1) their main documentary evidence (including electronic evidence) at the beginning of the process, with the statement of claim or response to the claim and (2) afterwards, only the relevant documents ordered by the Court upon request from the counter party after the case management hearing. In addition, there is a general obligation to preserve business documents for six years.

The final decision on how the process of collection, preservation and production of electronic information is done relies on the Court who will have to decide (1) upon the one party's request if the other party has to produce electronic information at all; (2) whether the information actually produced implies with the order issued at the case management hearing, and if not if it is admissible to order the production thereof, through the exceptional "diligencias finales;" and (3) the evidentiary weight of the fact that a party has not preserved crucial documents beyond the general compulsory term of six years or (there are specific cases where documents must be kept for shorter periods. For example, in the stock sales business the orders of sales or

purchases must be recorded and should be kept at least three years in the case of signed paper orders or electronic storage, and at least three months in the case of oral orders). For the assessment, the Court shall apply its reasonable discretion considering the availability of the evidence for the parties and the easiness to produce it.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

There are no privileged documents under Spanish law as understood in the common law systems. However, under certain circumstances, documents stored by lawyers could not be disclosed.

Lawyers are prevented to disclose certain matters. The profession of lawyer is governed in Spain by the Deontology Code, approved on 30 June 2000 (hereinafter referred as to DC), and the Royal Decree 658/2001 of 22 June, that enact the General Statute of the Spanish Legal Profession (hereinafter referred as to SLP). Article 1.2 of the SLP establishes: "2. During professional practice, Lawyers are subject to legal and statutory norms, to the loyal compliance of the rules and practices of the Bar professional deontology and to the resulting Bar disciplinary regime."

Article 5.2 DC, Professional Secrecy, states that the duty of professional secrecy includes the confidences and proposals of the client, of the contrary party and of colleagues as well as all facts and documents that we could be aware of or received as a consequence of his professional activity, while 5.3 DC provides that a lawyer cannot produce in Court and deliver to his client the letters, notes or communications received from the lawyer of the other party, unless he would be expressly authorized. Accordingly, Article 11.1.g), Relationships with the Courts, states that the lawyer shall not disclose or provide the Court with settlement proposals issued by the other party or his lawyer, unless expressly authorized.

SLP provides similar duties (Article 34.e), imposing to lawyers the obligation to not disclose conversations or correspondence with the other lawyer, prohibiting to produce such as evidence without authorization. SLP provides penalties for the infringement of these rules or deontology rules. Articles 84 to 86 SLP contain a range of actions that are regarded as contrary to deontology and the Statute. Disregarding very serious breaches, which would not apply in principle, the unauthorised disclosure of documents before the Courts could be subject to penalties of the Bar to the lawyer, ranging from suspension of the professional exercise to a warning in writing (*apercibimiento*), depending on how the seriousness of the conduct is regarded by the Bar. Moreover, the Bar penalties do not prevent the party for seeking damages.

Article 542 of the Organic Act of the Judiciary Power releases lawyers from declaring about facts and issues that they may know as a consequence of their professional activity (limited by the money laundering regulations under certain conditions. However, Article 371 CPA, states that witness may be released by the Court after the Court hears the arguments to keep secrecy. It is arguable that a lawyer may be released but in our experience we have seen sometimes judges trying to oblige lawyers to declare. In our opinion, Article 542 of the Organic Act of the Judiciary Power overrides Article 371 CPA.

Among the pre-trial disclosure, it is possible to order the entrance in a place where it is believed that the requested documents may be stored. If this place would be a law firm, the lawyers are entitled to call the Dean of the Bar to check that the professional secrecy is not affected.

Please note that only the lawyers, and not the parties, are subject to these limitations, thus if the communications are directly handled to or between the parties, it would be possible to produce them in Court, save for a settlement proposal.

The final limit is that no evidence shall be admitted if it has been obtained in breach of constitutional rights.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

According to Article 394 of CPA, the general rule regarding the defense costs is that the losing party pays the costs of the other party unless the court appreciates that the case presented serious factual or legal doubts. If the claim is admitted in part, each party pays its own costs and halves those common costs if any (*e.g.,* experts designated by the court). Cost are capped: they cannot exceed one third of the total quantum of the claim.

In any of the cases in which a party is entitled to receive form the other party the judicial costs, the costs of any means used to prove the authenticity of electronic evidence used, such as expert's reports, may be included within the said costs.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

There are not legal provisions regarding the use of legal hold notices sent by parties. The only available action is to apply judicially for the conservation of evidence, provided that the legal requirements are met (*see* question 3 above, conservation of evidence).

As we mentioned earlier, there is a general duty to preserve business documents for 6 years. This notwithstanding, there are some exceptions. For instance, non business related electronic documents in the hands of an appointed trusty third party should be preserved for a term of at least 5 years. Finally, the limitation period should be considered upon the action being brought. For instance, the general limitation period rule for contracts is 15 years as for tort, one year.

Apart from that, there are no general provisions from the public administration or material or procedural provisions regarding records management guidelines or general records retention schedules. Notwithstanding the foregoing, according Article 6.3 Civil Code there is a general duty to exercise rights in good faith, and the failing of one party to preserve electronic documents after a request from the counter party may have some impact in the Court's assessment of a case, as the court may deem that the one of the parties has not been acting with loyalty.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The electronic information management technologies are spreading in Spain. Thus, the ASISEC, with the purpose of providing a suitable legal framework which generates trust in internet use, created the legal status of "*trusted third party*". According to Article 25 of ASISEC, the parties to an electronic agreement can agree that a third party stores the declarations of will and the date and the hour of such communications. The trusted third party does not need to be a notary public, and will have to store the information for the period agreed by the parties, but no less than five years. This possibility will ease the procedural position in the event of a dispute, as it will help to prove that the information stored has not been altered.

However, the legal status is an impartial party whose object is to provide the maximum protection, safety, trust and guarantees to the e-commerce and all its users. Moreover, these services intend to favour and benefit the execution of agreements by electronic means. The services that this trusty third party can provide are: (i) to file and certify the content of the purchases, (ii) to file the on-line agreements and (iii) to file emails. For instance, the first service can be offered to online businesses, and these services provide maximum legal coverage to these businesses, as well as to its clients. Moreover, this service will increase the safety and trust of the user which will be beneficial to the on-line business. In the case of the service of filing online agreements, it offers the safety of storing the content of said agreements by a third impartial person. Finally, the storage service of emails consists

of verifying the notification that the party wishes to carry out, such as commercial communications, claims to companies, etc.

There are a few companies offering these services at the moment, and therefore the use of these services is still not widely used.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

According to Article 287 of CPA, evidence will not be valid if it is obtained with violation of constitutional rights. In this respect, a party may refuse to disclose the documents or evidence requested by the other, if those documents referred to a third party to the trial and are subject to a confidential business agreement or in any other way the rights (honor, intimacy) of the persons listed in those documents may be breached if the said documents are disclosed without their consent. The court will have to decide if the taking of that evidence does not violate the rights of third party to the trial, and therefore if the requested party has the obligation, despite his arguments of violation of privacy rules, to produce the requested documents. In this sense, it is possible that the court may articulate the means to avoid the impact of the disclosure to the third parties rights (for example, allowing the disclosure of just the relevant parts to the trial of a contract, keeping the rest of the contract secret to the parties to the trial).

Regarding electronic documents, please note that in general terms, the personal -not work related – use of computer facilities entrusted by the company to employees may generate conflicts with the exercise by the company of its right to control and supervised its business, and this may affect the constitutional rights of the employees regarding the respect for his private life and the secret of his correspondence in cases dealing with personal emails, internet navigation and certain personal files.

Recent case law[250] has established some limitations for the employer in his exercise of his right to control the use of computer and communications means provided to his employees. The resolution states that the employer, following the general rule that rights must be exercised in good faith, must (a) previously establish the rules of usage and a list of prohibited conducts in connection with the use of computers and telecommunications provided by the company and (b) advise the employees that control and supervision of the said means will be carried out and how this will take place. If the employer fails to give these warnings, then any information obtained from personal emails or personal files stored in the employees' computers will not be valid evidence in trial against his employees due to the violation of the constitutional right to privacy, and in the case of the emails, the right to secret of correspondence. Following the Decision of the European Court of Human Rights of 3rd April 2007 (Copland case), the Supreme Court clarifies in his decision that the protection or guarantee given by the constitutional right to privacy also covers the "information derived from tracking the personal access to internet," *i.e.,* without prejudice to what we have already said about the employer's warnings, the information from the temporary internet files is also protected by the right to privacy.

Regarding disclosure/production of documents in legal proceedings or regulatory enquiries commenced in other jurisdictions, any request would only be enforceable in Spain under the international regulations and treaties related to taking of evidence to which Spain is a party. Those laws and treaties are described under question 21.

[250] Decision of Labour Chamber of the Supreme Court of 26 September 2007, nº 966/2006, issued in a remedy of appeal to unify the legal doctrine on this matter.

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

The origin of Spanish data protection legislation is in first place the right derived from Article 18.4 of Spanish Constitution 1978 (SC) that states that "the Law shall limit the use of information technology to guarantee the honor and personal and family privacy of the citizens and the full exercise of their rights." In second place, we have to refer to the Council of Europe Convention 108 of 21 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which took force in Spain on 27 January 1984. The said convention set the guiding principles and rights that any legislation in any jurisdiction must have to protect personal data, and created for the Spanish legislator the necessity to pass a Data Protection Act, that was finally enacted in 1992 by Organic Act 5/1992 on the Regulation of Automatic Processing of Personal Data. The purposes of this Act were, as it was stated in the Preamble, to face the risks, that for the personality rights may involve the storage and processing of data by computer applied means. Consequently, the Act was applied only, following Article 18.4 of SC, to automatic files.

The approach that privacy had to be protected from information technology only was abandoned by the current Personal Data Protection Organic Act 15/1999 of 13th December (PDPOA). This Act implemented in Spain the EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Since the coming into force of PDPOA, the data protection rules in Spain do not deal with information technology only and apply to any processing, automatic or not, of personal data, performed either by individuals, private or public organizations. The PDPOA was further developed by the Royal Decree 994/1999 of 11 June approving the Regulation on security measures applicable to automated filing systems containing personal data.

The evolution cycle regarding the data protection was followed by the consideration of the right to data protection, following Decisions from the Constitutional Court number 290/2000 and 292/2000 both of 30 November, as fundamental right derived directly from the SC which is independent and autonomous from the right to personal and family privacy. Now the right to data protection is not only linked to Article 18.4 SC but is also directly connected with the respect to the person's dignity enshrined in Article 10 SC. To summarize it, the processing of personal data without the consent of the person concerned is just playing with the person's identities and, as a result, with their dignity.

This has its correspondence, at EU level, in Article 8 of the European Chart of Fundamental Rights, which provides the following principles that inspire the principles laid down in PDPOA:

- The right of every person to the protection of his personal data.
- The personal data have to be processed fairly for specific purposes on the basis of the consent of the person concerned or a legitimate basis laid down by the law.
- The right of everyone of access to data collected concerning him or her, and the right to have it rectified or erase.
- The compliance with these rules is subject to independent supervision by an independent authority (in the Spanish case, the Data Protection Agency, DPA).

PDPOA has developed the abovementioned principles, adding to the above the following principles: 1) the principle of accuracy and proportionality of the data collection process; 2) the principle of transparency and information of the data collection process; 3) the principle of specific categories of data with special protection and of non-discrimination in the use of the said data; 4) the principle of data security and of duty of secret of the data processed; and 5) the principle of responsibility of the controller in charge of the processing of data and the right of compensation when damages are suffered due to a violation of the PDPOA rules.

The most recent piece of legislation in the data protection area is the Royal Decree 1720/2007 of 21st December 2007 approving the Regulation implementing the PDPOA (Regulation). The said Regulation will enter into force on 19 April 2008. The principal objectives of the new Regulation is to provide more legal certainty and greater clarity to the practical application of PDPOA by 1) bringing coherence to the pre-existing frame work of secondary legislation (the Royal Decree 994/1999 is now repealed); 2) consolidating past decisions and precedents from the DPA and the courts in the area; and 3) addressing a number of issues that, during the years in which the PDPOA has been in force, were needed of express regulation.

The main developments brought about by the developing legislation are:

1. Clarification of the scope of application of PDPOA. Now, for example, it is expressly excluded the application of PDPOA to the processing of data relating to legal entities and files that merely include data of employees of these companies or the processing of data relating to individual traders that refer to such persons in their capacity as businessmen.

2. The controller must ensure that the persons concerned are able to exercise their rights of access, rectification or erasure by a straight forward mean totally free-of charge. Thus, any provision imposing the persons concerned the obligation to send, in the exercise of the abovementioned rights, a certified letter or suchlike will be null and void.

3. New security measures applicable to the processing of personal data. The Regulation takes a more vigorous approach to the assignment of the three levels of security (basic, medium, high) in terms of setting measures to be implemented in each case. Noteworthy, for the first time there is specific regulation of security measures for non-automated filing systems. Thus the new Regulation requires certain filing criteria to be applied to ensure the effective exercise of the rights to object processing. Further, filing cabinets, archives and other storage facilities must be equipped with appropriate locking devices to prevent unauthorized access to the documentation.

4. New requirements for the valid outsourcing of the data processing by the data controllers to processing agents.

5. Data processing of underage people. It expressly permits the processing of data related to minors[251] of or over 14 years with their consent, unless a specific law requires the consent of the parents or legal representatives. For the processing of personal data concerning minors of or under 13 years of age, the consent of their parents or legal representatives is required.

[251] The age of majority in Spain is 18 years old.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

Following Article 2 of EU Directive 95/46, Article 3 a) of PDPOA defines "personal data" as the "any information relating to an identified or identifiable natural person." This must be completed by the definition of the scope of PDPOA of Article 2, which provides that the PDPOA will be applicable to the personal data registered in physical means that may be subject to process and any subsequent use of those data by the private or public sector.

On its part, Article 3 (c) of PDPOA defines "processing" as:

> any operation or set of technical operations, performed whether or not by automatic means, that allow collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, blocking, erasure or destruction of data, including the assignment of data resulting from communications, consultations, interconnections and transfers.

In addition, the same Article defines "controller" as the natural or legal person that is responsible and sets the purpose, content ands use of the processing; "processor" as the natural or legal person that processes data on behalf of the controller; and "data subject" as the natural to whom belongs the data undergoing the processing.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

As above mentioned in the answer to question 19, according to Article 287 of CPA, evidence will not be valid if it is obtained with violation of the constitutional rights of honor, intimacy, respect for his private life and the secret of correspondence. In this respect, this was dealt under question 19.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

In both criminal and civil jurisdictions, the data protection and privacy legislation is applicable. In principle in both criminal of civil proceedings the court will have to decide if there are restrictions to disclosure/production of evidence due to data protection, privacy and other fundamental rights rules. If the court considers that the said rules are applicable then in principle the consent of the concerned party is required for the evidence to be valid.[252] However, in the investigation of criminal proceedings, the court may, under certain requirements, waive the applicability of the data protection and privacy rules and allow more intrusive searches of defendant's premises, person, possessions or communications.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

The data protection rules are not applicable to legal persons. As stated under the above 20(b), Article 3 defines personal data as any information concerning identified or identifiable natural persons.

[252] A reference to Article 11.2.(d) PDPOA, which does not require consent for the transfer to judicial authorities, may be appropriate in this context.

The new 2008 Regulation has tried to clarify and specify the applicable scope of data protection rules, and its Article 2.2 states that this Regulation is not applicable to the processing data relating to legal persons. In addition, Article 2.3 stipulates that the data related to individual businessmen will be excluded when they refer to them with status of merchant, industrialist or ship owner. Therefore, the personal data of said businessmen referred to their natural condition, out of their mercantile scope, are protected by the data protection rules.

A recent guideline has been issued by the Data Protection Agency (DPA) in this regard. The DPA has pointed out that the application of the PDPOA is excluded from the files in which the inclusions of identifying data of natural persons are included accidentally, in relation to the content or purpose of the processing. As an example, said guideline considers the Resolution of the DPA of 19 July 2005, which refers to the recording of a telephone conversation referred to a property purchase and held by the plaintiff, in his Company Director status, and by the Director of the defendant company. The plaintiff filed a claim before the DPA he considered that the protection of his personal data has been violated by this recording. However, the DPA concluded that as the scope of the conversation was referring to the exclusive framework of the plaintiff's activity (which consists of the construction, developing and property sale), the processing of the plaintiff's personal data was not included in the scope of applicability of the PDPOA.

In addition, the Resolution of 31 January 2007 closed the proceeding in which the object of the processing was only referring to the professional information of the plaintiff, given that the plaintiff's data had been obtained from the Mercantile Registry.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

Yes, there are some exceptions. On a general basis the files which do not require the protection envisaged in the PDPOA. As we stated in the foregoing question, these rules are not applicable to legal persons or individual businessmen in their status of merchant, industrialist or ship owner. In addition, the files containing the following data of natural persons that render their services to any legal persons – names and last names, the responsibilities and the rest of the professional data, as address, email, telephone and fax – are not included in the scope of applicability of the data protection rules.

The new introduction of the Regulation regarding the personal data of deceased persons should also be noted. Up to date, numerous doubts have been raised whether this data were also protected by the PDPOA. The Regulation sets forth the non-application of its rules to the data of deceased persons (Article 2.4). Notwithstanding, the persons linked to the deceased, for familiar or analogous reasons, may notify the death to the controller or processor of the files where the personal data of the deceased person were contained. In this regard, the justification of said death is necessary. The relatives may also require the cancellation of said data if possible.

In addition, Article 4 of the Regulation indicates the files and the processing excluded from the application of the data protection regime. There are three: (a) the processing relating to the private life and family activities of the individuals; (b) the files relating to classified material; (c) the files corresponding to terrorism investigations and criminal organizations. In this regard, the controller must previously communicate to the DPA the existence of said file, its purpose and its general features.

Along this line, the DPA issued the Legal Report 0000/2000 which deals with the processing by the attorney or procurator of the contrary parties' personal data in a judicial proceeding. Pursuant to the above report, the DPA answers whether the processing of said data could produce a conflict between two fundamentals rights: (i) the right to a due process of law that affects the attorney and procurator's clients and (ii) the right to protect the personal data of the contrary parties. The conclusion is that, within the scope of the proceeding, this processing of personal data will not require the previous consent of the data subject and the right to a due process prevails. However, the data protection rules apply in full to attorneys and procurators if they carry out the process of these data for purposes out of framework of the judicial proceeding.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

There are no provisions that specifically envisage the restriction of the electronic discovery of specific data types, subject areas or situations, but the PDPOA considerations regarding the processing of data with special protection must be considered on general basis.

The PDPOA regulates this kind of data in its Article 7, as data named "*specially protected*." PDPOA grants this category a major level of protection and special obligations are also required, such as the need to obtain the express consent of the data subject. This data subject shall also be warned of his right to refuse such consent. It should be noted that this requirement is directly based on the SC.[253]

Pursuant to Article 7 of PDPOA, this category is composed of personal data referring the ideology, religion, beliefs and trade union membership, racial origin, health or sex life of the affected subject. This Article also refers to personal data that the competent public administrations may include in their files, such as personal data on criminal offence or administrative infringements.

It should be noted that the violation of the duty of secrecy on personal data with special protection without the express consent of the affected persons will be deemed as a very serious infraction pursuant to Article 44.4.(g) of PDPOA (infractions are classified as minor, serious and very serious) and fines for serious infractions rage from €300,000 to €600,000.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

This question has been answered in the above question 19, and is also completed in question (k) below.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

This role is carried out by the DPA whose general functions is to watch over the fulfilment of the data protection rules and the control of their application.

As the protection data rules affect data subjects as well as those who process personal data, the activity of the DPA is carried out by two means. In relation to the former, DPA attends to their requirements and complaints and to inform the relevant persons regarding their legal rights in this matter. In relation to the latter, basically DPA issues the corresponding legal authorizations, requires the adoption of correction measures, deals with the administrative authority to impose the

[253] Article 16.2 of SC states that nobody may be obliged to declare his/her ideology, religion or beliefs.

administrative fines and authorizes the data international transfers. Moreover, this is the authority in charge of informing regarding the bill of developing rules of the PDPOA, and issuing guidelines and introductions in this matter.

Within the DPA is highlighted the role of the General Registry of Data Protection ("the Registry"). This Registry is in charge of the registration (i) of the public administration and private company files, (ii) of the international authorizations of data transfers (iii) of the standard codes of conduct. In addition, PDPOA requires it to publish periodically the list of the registered files. According to PDPOA, its Regulation rules the registration proceeding of the files as well as the content of the entry, its modifications, cancellation, complaints and appeals against the corresponding decisions, and other related matters.

With said functions, the Registry develops the publicity principle with the purpose of providing the citizen the exercise of the right to obtain information from the Registry regulated in Article 14 of PDPOA. This information shall be provided in a public and free manner by the DPA's website. In this regard, the DPA is working on improving the information service of its website with the aim of extending the information of the registration and maintaining its online update.

It should be noted that the registration is required with the purpose of making the data processing legal, but this registration is, indeed, a mere declarative act. Therefore, non-registration is contrary to PDPOA, although to be registered does not mean that the data processing is totally in accordance with the law.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

Sections 33 and 34 of PDPOA deal with regime to be observed for international transfers or movements of data. Said provisions have been developed by DPA's Instruction 1/2000 (part of which were declared void by the Supreme Court in its judgment of 25 September 2006) and by the new Regulation of PDPOA.

The first rule is that international transfer of data does not exclude the application of the provisions of PDPOA to the controller which intends to transfer or transfers data outside Spain.

Regarding the procedures, the regulations set two different procedures as a general rule:

- *Transfers of data to countries that provide an adequate level of protection.*

  The Director of the DPA will asses which countries present an adequate level of protection, and a list of those countries will be issued by the DPA. Transfers of personal data to those countries will not be required to request a prior authorization. The same applies to transfers to countries which the Commission of the European Union, in the exercise of its powers, has declared that they ensure an adequate level of protection.

  Notwithstanding the foregoing, the DPA may allow to the temporary suspension of the international data transfer to a recipient located in a country declared to provide an adequate level of protection when: 1) the supervisory authority of the country of destination, rule that the recipient has breached the data protection rules of their national law or 2) there is prima facie evidence that the recipient is in breach of the rules of data protection and the

supervisory authority of the destination country have no adopted or is not in future going to take any measure to resolve the case in question regardless the DPA warnings about the situation.

- *Transfers of data to countries that do not provide an adequate level of protection.*

  These type of transfers are subject to prior authorization by the Director of the SPDA.

The recent Regulation of PDPOA admits the possibility of authorization of international transfers of data within multinational groups of companies, where such groups have adopted the same binding corporate rules which provide the necessary safeguards respecting the fundamental right to data protection and the provisions of PDPOA and its implementing Regulation.

Finally, among the exceptions to the general rules described above, Article 34 of PDPOA provides that the data transfer may take place regardless the need of prior authorization where: 1) the transfers are necessary in order to protect the interests of the data subject in a contract between the data subject and the controller or the controller and an third party 2) the transfer serves the purposes of offering or requesting international judicial aid as a result of applying international treaties to which Spain is a party, or the transfer is necessary for the recognition, exercise or defence of a right in legal proceedings.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

No prior consent is required for the processing in countries that provide an adequate level of protection.[254] Pursuant to Article 6 of PDPOA, the data subjects' consent is not required where the personal data related to the parties of a contract or preliminary contract for a business, employment or administrative relationship, and they are necessary for its maintenance or fulfilment. Therefore, if the personal data collected are used outside of the employment context (such as the sending of commercial publicity to employees) the company is obliged to require the consent of these employees. In addition, employee's consent will be required after finishing the contractual relationship, in the event that the company wants to carry out the processing of the personal data of the former employee.

Notwithstanding and before hiring an employee, the companies shall inform their employees of the data collection according to Article 5 of PDPOA. In this regard, the company shall inform about at least the following information: (i) The file's existence; (ii) the purpose of the data collection, (iii) the information transferees if any; (iv) the access, modification and cancellation rights of the affected person; (v) regarding the address and identity of the controller. The PDPOA does not establish how to provide the above information, although it would be indicated in the employment contract.

The companies shall also comply with the duty of secrecy envisaged in Article 10 PDPOA and must fulfill said rule even after the contractual relationship is concluded.

The Criminal Code also governs this duty in Article 197 provided that the violation breaches the privacy rights, the image rights, and the inviolability of the private property. This refers to the appropriation of any personal secret of the employee or the disclosure of personal communications without the employee's prior consent. It should be noted that for the perpetration of said offence is

[254] The employee's consent will be necessary for the processing of his/her personal data by the employer in non-adequate countries (unless an exception applies, or the employer obtains an authorization from the DPA). The employee's consent will be necessary for the transfer of his/her personal data by the employer to any third party, unless the third party is a data processor providing a service to the employer or a legal exception applies.

necessary the existence of two elements: (i) an objective element as the use of a recording system or reproduction system of the sound or image and (ii) a subjective element relating to the purpose or intention of disclosing the employee secret or violating the private life of the employee. The violation of this right is punishable with imprisonment of three to five years, but if the information disclosure by the company refers to sensitive data such as the ideology, religion or sexual life of the employee, the penalty envisaged will be greater, imprisonment of four and a half to seven and a half years.

In addition, the non-fulfilment of personal data rules in this regard by the company may be sanctioned by the DPA, which will be deemed as a serious infraction.

Cross-border Discovery

21. *Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:*

    a. *Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.*

    b. *If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.*

    c. *What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?*

    Spain is part of several international Conventions and bilateral agreements on this matter:

    The Council Regulation (EC) 1206/2001, of 28 May 2001, on cooperation between the Courts of the Member States of the European Union in the taking of evidence in civil and commercial matters

    It should be noted that in accordance with Article 249 of the Treaty establishing the European Community, the Regulation is directly applicable in all EU Members States, with the exception of Denmark, which opted out, and prevails over other provisions contained in bilateral or multilateral agreements or arrangements concluded by the Member States.

    The Regulation provides two basic means to gather evidence in civil and commercial matters (criminal, tax and administrative matters are excluded): (a) requests to the competent court of another Member State to take evidence or (b) to take evidence directly in another Member State. In both cases procedural requirements set forth in the Regulation must be met (form and content of the request, language, etc.).

    In relation to the requests to the competent court of another Member State, the general rule is that the requested court shall execute the request in accordance with the law of its Member State, but upon request by the requesting court for the request to be executed in accordance with a special procedure provided for by the law of its Member State, the requested court shall comply with such a requirement unless this procedure is incompatible with the law of the Member State of the requested court.

    The request can be directly addressed to the competent court of the other state, although the central body designated by that state will be responsible to give advice to the competent courts and provide solutions in the case any difficulties arise. Moreover, the parties may be present in the performance of the evidence in the event the law of the either the requesting or requested court allow it. Further,

legal representatives of the requesting court may be also present in the performance of the evidence in the event the Law of the requested court admits it.

In relation to direct taking of evidence by the requesting court, it is only admitted (1) if it can be performed on a voluntary basis without the need for coercive measures; (2) if it meets the procedural requirements set forth in the Regulation; and (3) if it is not contrary to fundamental principles of law in the requesting court Member State. The taking of evidence shall be performed by a member of the judicial personnel or by any other person designated in accordance with the law of the Member State of the requesting court. Please note that the competent authority of the Member state where the evidence is going to be taken may assign a court of its state to take part in the performance of the taking of evidence in order to ensure the proper application of the provisions of the Regulation.

The Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters of 18 March 1970 (hereinafter referred to as "the 1970 Convention")

It took force in Spain on 21 July 1987. Therefore, a Spanish court should accept any request from any other party to the 1970 Convention presented in compliance with its rules.

The 1970 Convention sets forth two different ways for taking evidence abroad: (i) Letters of Request, which implies the direct petition from a jurisdictional body to another based in another contracting State; and (ii) the taking of evidence by diplomatic officers, consular agents and commissioners.

Letters of Request: Should comply with the requirements stated in Article 3 and should be drafted in Spanish or translated into it (Spanish reservation to the Convention). If the requesting foreign judge or any official appointed by said judge would like to be present, prior authorization from the Spanish authorities is required, according to the reservation allowed by Article 8. Article 9 of the 1970 Convention states that the judicial authority executing the letter of request shall apply its own law regarding methods and procedure.

Finally, it should be noted that according to the reservation allowed by Article 23, Spain does not accept letters of request regarding the procedure known in common law countries as "pre-trial discovery of documents."

Taking of evidence by diplomatic officers, consular agents and commissioners: Diplomatic officers and consular agents may take evidence in Spain from their own nationals. Spain has made no declarations to the contrary nor has it imposed any restrictions. No prior authorization from the Spanish authorities is required for diplomatic officers, consular agents or commissioners to take evidence in Spain without compulsion of Spanish nationals, as Spain has not declared that such authorization should be sought for. Evidence should be taken in the Embassy or Consulate of the requesting State. Pursuant to Article 18 of the 1970 Convention, diplomatic officers or consular agents may request the collaboration of the Spanish courts in the event that compulsion would be necessary. This request should be made to the relevant authority, which is the Secretaría General Técnica del Ministerio de Justicia.

Other Treaties

Spain is a party to The Hague Convention on Civil Procedure of 1 March 1954, which took force in Spain on 13 December 1961. The 1954 Convention has been replaced by the 1970 Convention between the Contracting States of both Conventions and it is still in force between Spain and those

States that are not a party to the 1970 Convention.

Further, Spain is a party to the Inter-American Convention on judicial assistance and letters rogatory, of 30 January 1975, since 15 August 1987. This Convention establishes the same procedure for the service of proceedings and the execution of Letters Rogatory aiming at obtaining evidence abroad. The procedural laws of the recipient state apply, while special procedures are accepted, provided that they do not infringe upon the public policy of the recipient State.

Additionally, Spain has entered into bilateral treaties for the taking of evidence abroad with several States: Czech Republic and Slovakian Republic, Brazil, China, Bulgaria, Morocco, Russia, Thailand, Tunisia, Algeria, Mauritania and the Dominican Republic.

Regarding discovery in criminal matters, Spain is a party to the Convention on Mutual Assistance on Criminal Matters between the Member States of the European Union of 29 May 2000 and some bilateral Treaties.

Switzerland

Christian Zeunert - ***Lead Editor***
Roberto Dallafior, Claudia Goetz, Thomas Mueller, Alois Rimle - ***Contributing Editors***
David Rosenthal - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   Switzerland is a *civil code jurisdiction*. The competence to enact law is split between the Swiss Confederation and the 26 cantons. Whilst the Swiss Confederation legislates in the field of substantive civil law, the cantons are competent to enact their own code of civil procedure and judicial organization. However, some provisions of federal statutes and some decisions of the Federal Supreme Court include procedural rules which take precedence over cantonal procedural law.

   Given the power of the cantons to enact their own code of judicial organization, each of the cantons has its own court organization. All cantonal courts administer both cantonal and federal law. Litigation generally is initiated in a cantonal court. Both the courts of first and of second instance are cantonal, while the highest court, the Swiss Federal Supreme Court, is federal. In civil litigation, the Swiss Federal Supreme Court normally decides appeals against cantonal court judgments. In Switzerland, the judiciary therefore is *multi-tiered*.

   In Switzerland, the law relating to document disclosure is *governed by statutory provisions* and not by case law. Because of the described separate competence of each canton to enact a code of civil procedure, there are no uniform rules relating to document production.

   On the basis of the revised Federal Constitution, a bill on a new Federal Code of Civil Procedure has been presented. Such Federal Code of Civil Procedure is to replace all cantonal codes of civil procedure. It is expected that the new Federal Code of Civil Procedure will be enacted in 2010 or later. An excerpt of the Code of Civil Procedure of Zurich ("Zurich Code") and an excerpt of the draft of the Federal Code of Civil Procedure ("Draft Federal Code") relating to the gathering of evidence is attached hereto. Some provisions of the Draft Federal Code might be changed by the Parliament.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   For a better understanding of the following comments, it might be useful to recall three fundamental differences in the approach to civil proceedings in countries with a so-called civil law system[254] as opposed to countries with a so-called common law system.

   First, proceedings under the regime of a civil law system start with extensive pleadings; generally the parties submit two rounds of submissions setting forth all relevant facts in great detail. The evidence gathering

[255] Simply put, this term is meant to describe proceedings as organized in countries with a civil law system as, for example, continental Europe and Latin America.

including the hearing of witnesses and the production of documents requested by the other party is for the second stage of the proceedings.

Second, the gathering of evidence is considered to be an act of sovereignty and is, therefore, reserved for the state authorities. The parties and their representatives are not entitled to gather evidence being considered as act reserved to authorities. As an example, it is a prerogative of the judge to question the witnesses. The parties' representatives are prohibited from contacting the witnesses prior to the hearing. The judge will ask questions with respect to the facts pleaded by the parties in their submissions. The parties may be present at the hearing and may ask additional questions that, however, require the court's leave.

To prevent the gathering of evidence from being performed by non-authorised individuals or foreign authorities on Swiss territory, the Swiss Penal Code (SPC) provides in Article 271 that whoever performs acts for a foreign state on Swiss territory that are reserved to an authority or an official without being authorised to do so shall be punished with imprisonment (see hereafter under question 21(b)).

Third, in proceedings in a civil law system each party must build its case on the basis of documents in its possession. The production of documents by the opposing party is the exception to this rule. The documents are, if at all, produced during the evidence gathering, *i.e.,* during the second stage of the proceedings.

Because the gathering of evidence is reserved to be performed by the State authorities, there is *no automatic obligation to disclose or produce documents* absent a court order (see Zurich Code § 183). In Swiss proceedings there is no "discovery phase" as such. A procedural duty to produce documents generally arises only at the *evidentiary stage* of a court proceedings, *after the pleadings* are completed, *i.e.,* after the exchange of briefs (statement of claim, answer to the complaint, reply and rejoinder). Therefore, and this is one of the most important differences between a Swiss proceeding and, for example, a U.S. proceeding, a request for document production cannot be used to establish the factual basis for the claim before the commencement of an action.

Hence, a party is obliged to produce documents *only at the order of the court*. A court will order the production of documents only when it deems production necessary. The court must be satisfied that (1) the requesting party and the opposing party have pleaded the factual circumstances in sufficient detail, that (2) the factual circumstances invoked are material and relevant to the case and that (3) the request is clear and specific so that the document can be identified (see Zurich Code § 136, 137). For all these reasons, in a Swiss proceeding, document production is generally *quite limited*.

The duty of producing documents normally lies with the party in whose possession or custody or under whose control the relevant documents exist. Third parties are obliged to submit documents to a court unless they are entitled to refuse testimony. The opposing or a third party's legitimate interest may limit the duty to produce documents. They may, for example, invoke that a document is privileged.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Two different problems must be distinguished: First, the question whether a party can ask for the production of documents before the pleadings are completed, and second, the question whether a party may request that evidence be preserved before an action is commenced.

(1) As mentioned, an obligation to produce documents normally arises only at the evidentiary stage of court proceedings (see above question 2), once the pleadings are completed. Hence, a party (or third party) may be obliged to produce documents before that stage of the proceeding if such duty is based on an obligation under the applicable *substantive law*.

(2) Before an action is commenced, the court may gather evidence upon a request of a party if the requesting party (i) has a claim (on the basis of substantive law) that the facts be rapidly established or (ii) can make a *prima facie* case that the evidence gathering would become impossible or extremely difficult if delayed.

During such proceedings the court may take such measures as necessary to preserve evidence (see Zurich Code § 135, § 155). The draft of the Federal Code provides that the court may take evidence at any time if the law provides for a valid claim to that effect or if the requesting party can show that it has an interest that is worth being protected or can plausibly claim that the evidence is at risk.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

While the parties have no general legal obligation to preserve documents with regard to a proceeding, a party shown to have destroyed a document runs the risk that the competent court will *draw negative inference* from such behavior (see Zurich Code § 148).

The Swiss Code of Obligations, however, states in Article 963-1 the following as regards documents subject to a legal preservation requirement:

> In case of litigation on matters connected with the business, those who are obligated by law to keep books may be ordered to produce the books, business correspondence and accounting records if an interest worthy of being protected is proven and if the judge deems the production of such records necessary for evidentiary purposes. Businesses are in general required to retain their books, accounting records and business correspondence for a period of ten years, following the respective fiscal year (Articles 957, 962 of the Swiss Code of Obligations).

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

Generally, there are *no provisions for sanctions* if a party fails to preserve documents in the cantonal codes of civil procedure. However, if a third party having an obligation to cooperate disobeys without justification, the court may impose fines up to CHF 1'000 or order the sanctions according to Article 292 Penal Code or order the implementation by force (*see* Draft Federal Code Article 164). If the court issues an order to preserve and provide evidence under the sanctions of Article 292 Penal Code, the party not complying with this order can be sanctioned with detention or fine.

It should be mentioned in this context that the violation of the general obligation to retain books, accounting records and business correspondence may be fined (Article 325 SPC).

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

Since document production in a Swiss court proceeding is fairly limited (far less extensive and voluminous than document production in a U.S. court proceeding), *costs are not excessive*. Costs of document production are not compensated separately; compensation for costs is normally awarded in the final order, judgment or award according to an official schedule that determines the costs depending on the amount in dispute. Costs for civil proceedings follow the event, *i.e.,* are usually borne by the non-prevailing party (*see* Zurich Code § 64, 68).

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

   There are currently *no legal provisions* specifically relating to the production or disclosure of electronic documents in civil proceedings.

   The current Draft Federal Code defines the term "document" as including electronic files (Article 174).

   In general terms, electronic documents as evidence are admissible (Art. 8 ZGB, Art. 29 Abs. 2 BV, Art. 6 EMRK, Draft Federal Code 147). Depending which cantonal law is applicable, an electronic document belongs to the evidence category instrument (*Urkundenbeweis*) or inspection (*Augenscheinbeweis*).

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

   There is no general definition of "electronic document" or "electronic data." However, Article 963-2 of the Swiss Code of Obligations appears to be relevant in this context. It states the following:

   > If books, accounting records and business correspondence are stored electronically or in a similar form the court or the authority entitled to require the disclosure based on public law may order that (a) the documents are presented in a way that they can be read without devices or (b) the devices necessary for reading the documents are provided.

   The probative force of electronic documents, especially e-mails, is uncertain since electronic documents can be easily manipulated. The court will decide whether or not it will accept emails as documents with probative effect. When assessing the probative effect, the court is not bound by specific rules but is free to act at its own discretion. The court is free to appreciate the evidence. In this context please take note of the following rule in Article 957-4 of the Swiss Code of Obligations that applies in cases where documents are stored in electronic form as specified in the Swiss Code of Obligations (Articles 957-963) and the Ordinance regarding the Keeping and Storage of Business Records: It states that books, accounting records and business correspondence that are stored electronically or in a similar form have the same probative force as documents that can be read without devices.

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

   There is no rule in Switzerland for the parties to directly "meet and discuss electronic disclosure." However, the parties are free to meet and discuss any electronic disclosure of data in their possession. All steps for evidence taking have to be handled and ordered directly from court. A party might ask the court to order evidence taking.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

    Civil Procedure laws in Switzerland usually have rules to prevent the destruction of evidence in pending litigation.

    The court can, on request of a party, impose adequate measures to safeguard evidence in case there is a danger that such evidence could be destroyed by the other party.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

    There is no general legal provision or rule that specifies the scope of a party's obligation to search for, disclose and produce electronic documents unless a court may order particular evidence. But the parties have an obligation to co-operate with the court in evidence taking (ZPO, § 157 b). The party may have the right of refusal (Federal Code ZPO, § 160). In case it is a false refusal the court can consider this in the evidence taking process (Federal Code ZPO, § 161).

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

    Not specified.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

    Please see answer to question 8.

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

    Not specified.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

    Not specified.

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

    Please see answer to question 6.

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

    Swiss law includes requirements to ensure the preservation of information for business and legal purposes, including in particular Articles 957 and 962 of the Swiss Code of Obligations, which requires businesses to retain books, accounting records and business correspondence for a period of ten years. Many companies may still store all relevant information in physical form, including emails (if at all). Some companies store certain relevant information in electronic form only. Companies in Switzerland are under a legal obligation to ensure (in particular by means of internal policies and/or procedures) that the preservation requirements under Swiss law are complied with, independent from whether the relevant information is stored in physical or electronic form. Please note that Swiss law includes specific requirements for the legally recognized preservation of electronic information.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

    Forensic specialists, investigation offices, law enforcement, and larger law firms are using such technology for gathering evidence. For Swiss based non-multinational corporations there may not yet be widespread use of

electronic information management technologies in Switzerland to assist with the preservation, classification, and management of electronic information for legal reasons. However, this may change in the future.

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

    Please see question 20(c).

Electronic Data Protection and Privacy

20. *Please describe your country's approach to electronic data protection and privacy. Please include in your response:*

    a. *The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)*

       The Swiss data protection legislation serves the purpose of protecting the personality and the fundamental rights of those persons about whom data are processed according to Article 1 of the Swiss Federal Act on Data Protection (Swiss Data Protection Act, DPA). The processing of personal data must generally take place in accordance with data protection principles specified in the Swiss Data Protection Act. The main data protection principles are the principle of lawful data processing, the principle of good faith, the principle of reasonableness, the principle of earmarking for specific purpose, the principle of data accuracy and the principle of data security (Articles 4, 5 and 7 DPA).

       Also, the Swiss Data Protection Acts includes transparency rules. Article 4-4 DPA requires that the collection of personal data and, in particular, the purpose of its processing is evident to the data subject. Article 7a DPA includes a specific information duty in situations where sensitive personal data and/or personality profiles are collected for inclusion in a data file.

       Furthermore, there are provisions designed to ensure that personal data are adequately protected when disclosed to a recipient in a country without legislation guaranteeing adequate data protection, unless one of the few defined exceptions applies (Article 6 DPA).

       Finally, additional data protection restrictions exist towards employees and can be found in employment law (in particular Article 328b of the Swiss Code of Obligations).

    b. *The legal definition of "personal data" and "processing" of data within your jurisdiction.*

       "Personal data" is defined under Swiss data protection law as "all information relating to an identified or identifiable person" (Article 3 lit. a DPA). Such definition not only included information relating to individuals but also information relating to legal entities. "Processing" is defined under Swiss data protection law as "any operations relating to personal data, irrespective of the equipment and procedures used, and in particular the collection, storage, use, modification, communication, archiving or the destruction of data" (Article 3 lit. e DPA).

    c. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

       Each party is obliged to produce such documents if so requested by the court; if a party does not comply with such obligation, the court may draw negative inferences. Please note in this context that

Swiss data protection law does not apply to the following legal proceedings in Switzerland: pending civil, penal, or international legal assistance proceedings (in Switzerland), or public or administrative law proceedings (in Switzerland) with the exception of administrative proceedings of the first instance (Article 2-2 lit. c DPA).

Third parties must also produce documents in their possession except if they can claim that they *have a right to refuse to give testimony*. If the parties cannot be compelled to give testimony, they are not obliged to produce documents, either.

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

Please see answer to question (c) above. However, the applicable procedural rules typically contain provisions geared towards protecting the privacy of persons and confidentiality of certain information.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Natural and legal persons have rights under Swiss data protection legislation if their data is processed by another person. They have a right of information towards the person controlling the data file (Articles 8, 9 and 10 DPA). They have also a right to file a (tort) claim before a civil court against any private person infringing upon their personality without sufficient justification, and request that their personal data are corrected or destroyed, or that the disclosure to third parties be stopped (Article 15 DPA).

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

Apart from the exception mentioned here above under (c) and (d), Swiss data protection law is not applicable in the following cases: personal data that are processed by a natural person exclusively for personal use and that are not disclosed to a third party; deliberations of the Federal Parliament and Parliamentary Committees; public registers relating to private law matters; and personal data processed by the International Committee of the Red Cross.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

Swiss data protection law does not include restrictions specific to electronic discovery. Instead, the general provisions of Swiss data protection law apply, and may well restrict the types of data or the situations in which electronic discovery is permissible.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

Swiss labour law includes a particular data protection rule for employee data. According to such rule the employer is permitted to process data of an employee (other than in his or her favour) only if such data processing concerns the qualification of the employee for the employment contract or if necessary for the performance under the employment contract (Article 328b of the Swiss Code of Obligations). Such mandatory rule applies also to the processing of employee data in the context of discovery.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The Swiss Data Protection Act includes transparency rules. Article 4-4 DPA requires that the collection of personal data and, in particular, the purpose of its processing is evident to the data subject. Article 7a DPA includes a specific information duty in situations where sensitive personal data and/or personality profiles are collected for inclusion in a data file. Furthermore, Swiss data protection law includes rules requiring that certain data processing is notified to the Swiss data protection authorities (Article 11a DPA). Finally, certain cross-border data transfer agreements must under certain conditions be disclosed to the Swiss data protection authorities (Article 6-3 DPA).

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

There are few established procedures in Switzerland for obtaining information in the context of litigation or investigations (*e.g.,* Swiss Federal Act on International Legal Assistance in Criminal Cases). Usually, a case by case analysis is required, also taking into account other critical provisions of Swiss law (*e.g.,* Article 271 Swiss Penal Code and secrecy obligations).

It should be mentioned in this context that the Swiss Data Protection Act includes general rules for the cross-border transfer of personal data (Article 6 DPA).

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

Employee consent may often not be a valid justification for the processing and transfer of personal data in the context of discovery under Swiss data protection law. Article 4-5 DPA states that if the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

Switzerland has ratified the Hague Convention. It is applicable in Switzerland. In general, collecting evidence in the context of a legal proceeding abroad is considered as a task exclusively of authorities and courts under Swiss procedural law. Swiss criminal law includes a provision (Article 271 SPC) that prohibits acts for a foreign state, in particular the collection of evidence in the context of a foreign civil procedure (see "blocking statute" under question (b) hereafter). The independent collection of evidence by a private person in the context of a foreign proceeding or investigation may be permitted to a limited extent only outside of the scope of Article 271 SPC.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

The provision of Article 271 of the Swiss Criminal Code is relevant in this context. According to Article 271-1 Swiss Criminal Code (1) whoever, without being authorized, performs acts for a foreign state on Swiss territory that are reserved to an authority or an official, (2) whoever performs

such acts for a foreign party or another foreign organization or (3) whoever aids and abets such acts, shall be punished with imprisonment up to three years or a fine and, in serious cases, with imprisonment not less than one year.

It follows that a deposition taken by private persons, *e.g.,* an attorney, is illegal. Permission by the deposed person or by any third parties affected will not relieve the deposing party from its obligations under Article 271 SPC. Also, if someone participates in an inspection or investigation of a company's files in Switzerland undertaken by representatives of a foreign authority, that person may violate Article 271 SPC.

The independent collection of evidence by a private person in the course of a foreign proceeding or investigation does not qualify as criminal act in accordance with Article 271-1 of the Swiss Criminal Code if an authorization is granted by the competent Swiss authorities. In the past various authorizations were granted to international companies with operations in Switzerland. For example, the Swiss Federal Finance Department granted an authorization under Article 271-1 of the Swiss Criminal Code as regards the cooperation with US authorities in the area of QI-taxation. It is also possible to obtain an authorization to undertake depositions on a case by case basis, provided, however, that the deposed persons participate voluntarily.

Article 271 SPC applies to acts that are reserved to an authority or an official. Such provision, however, does not apply to private arbitration procedures, provided that the arbitration tribunal is independent from government institutions. Furthermore, such provision does not apply to parties providing their own documents as evidence in a legal proceeding abroad. The parties are entitled to voluntarily provide evidence by filing own documents for the purpose of improving their procedural position. It is the Swiss authorities' view, however, that Article 271 SPC applies if a party has been ordered to produce certain documents. It needs to be determined on a case by case basis what documents qualify as "own" documents in the context of Article 271 SPC.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The relevant factors for permitting cross-border discovery may not always be the same as the competent Swiss authorities are generally different depending on the industry concerned.

Dealing with cross border discovery requests is a complex and not easy to balance challenge for multi-national groups of companies with operations in Switzerland due to data protection and other law restrictions. Swiss law restricts the gathering of potentially relevant information, both for internal investigations and for foreign court proceedings. Swiss data protection law (other than the data protection laws of most EU member states) applies not only to data of individuals but also to data of legal entities. If personal data are made available to a country without legislation guaranteeing adequate data protection, Swiss law (like the law of all EU member states) permits the cross-border data transfer only if an adequate level of data protection is ensured in the relevant country or one of the few defined exceptions apply (Article 6 DPA). The access to e-mail files of employees is particularly restricted in companies where employees are allowed to use the corporate e-mail system for private e-mails. Furthermore, personal data in contracts may additionally be protected by contract confidentiality obligations. Moreover, the disclosure of personal data in e-mails may generally need a legal justification (*e.g.,* justified by overriding business interests) and in case of cross-border disclosure an adequate level of data protection in the recipient country must be ensured under Swiss data protection law.

The gathering of potentially relevant information for internal investigations or foreign court proceedings may not only be subject to Swiss law but also to laws of other countries, if the headquarters of an international group of companies is located in Switzerland and the e-mails of group companies of various countries are concerned.

As a conclusion, the handing over of entire mailboxes to an U.S. outside counsel in the context of U.S. legal discovery will generally not be possible due to various restrictions under Swiss and possibly other laws. A feasible approach for disclosure purposes is to hand over only a filtered relevant subset for the specific case, and to implement certain procedures and contracts (or binding rules) to protect the privacy of the persons affected.

United Kingdom (England & Wales)

Janet Lambet - ***Lead Editor***
Neil Mirchandani, Clive Freedman, Quentin Archer - ***Contributing Editors***
Stewart Room - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   For many purposes the United Kingdom may be described as a unitary state, since there is no structure of federalism. However, whilst the legislative competence of the Parliament extends to all the United Kingdom, three distinct legal systems exist, each with its own legal profession, namely, England and Wales, Scotland and Northern Ireland. The legal systems of England and Wales are based on the common law.[256]

   Civil litigation brought in the courts of England and Wales is governed by the rules outlined principally in the Civil Procedure Rules ("CPR") and the practice directions accompanying the CPR, with disclosure issues covered by Part 31 of the CPR and the Practice Direction to Part 31. Case law has also been used to develop and apply the rules in CPR 31.

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   There is no provision under the CPR for automatic disclosure. The duty to disclose documents arises if and when, and to the extent that, the court orders disclosure. The usual order is that the parties must give disclosure (but not necessarily production) of the documents on which they rely, and the documents which adversely affect their own case, adversely affect another party's case or support another party's case, and the documents they are required to disclose by a relevant practice direction; defined as "standard disclosure" (CPR 31.6). However the court may, where appropriate, order wider disclosure.

   A party is required to make a reasonable search for standard disclosure (CPR 31.7) but the duty of disclosure is limited to documents which are or have been in a party's control (CPR 31.8).

   The opposing party then has the right to inspect and make copies of any disclosed document, unless the document is no longer in the control of the party who disclosed it, the party disclosing the document has a right or duty to withhold inspection of it on the grounds of privilege or the disclosing party considers it disproportionate to the issues in the case (CPR 31.3).

   There is no provision in the CPR as to when disclosure should happen. It can arise either from an agreement between the parties or as a result of an order of the court. The court will usually set a timetable for disposing of a case at a Case Management Conference ("CMC"), and will then provide for disclosure to be given by service on the other parties of a list of the documents that are or were in a party's possession or control.

[256] Scotland adheres to a unique judicial tradition which combines elements of the civil law of ancient Rome and the medieval common law of England. Northern Ireland is a common law jurisdiction and disclosure of documents in litigation in Northern Ireland takes place largely in accordance with the practice in England and Wales before the CPR were implemented in England in 1999.

It should be noted that the Commercial Court recently set up a Working Party to review the procedures used in long and complex trials. One of the recommendations of that Working Party, to deal with the administrative burden and cost of disclosure in large scale litigation, was that disclosure should not take place until after a CMC is scheduled to deal with disclosure. The Working Party also recommended that, in advance of the CMC, the parties should prepare a schedule identifying the disclosure required by reference to the issues in the case. The aim of this schedule is to control disclosure on each issue by reference to the classes of document, periods of time and level of disclosure that are proportionate to the costs involved and the likelihood of the disclosure assisting the court in determining the issue. The Working Party's recommendations are being run currently by the Commercial Court as a pilot, but it is expected that, in appropriate cases, the recommendations as to disclosure will continue to be the practice of the Commercial Court.

The duty of disclosure continues until the proceedings are concluded, and if additional disclosable documents come to the party's attention at any time, there is a duty to notify the other party of their existence (CPR 31.11).

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

Under CPR 31.16 a party may on application to the court, under section 33 of the Supreme Court Act 1981 or section 52 of the County Court Act 1984, seek disclosure before proceedings have started. The court may make an order under this rule only where the respondent is likely to be a party to subsequent proceedings, the applicant is also likely to be a party to those proceedings if proceedings had started, the respondent's duty by way of standard disclosure would extend to the documents or classes of documents of which the applicant seeks disclosure, and disclosure before the proceedings is desirable in order to (i) dispose fairly of the anticipated proceedings (ii) assist the dispute to be resolved without proceedings, or (iii) save costs.

CPR 31.17 also allows for an application for disclosure to be made to the court, under Section 34 Supreme Court Act 1981 or Section 53 of the County Courts Act 1984, by a person who is not a party to the proceedings. The court may make an order for disclosure against a non-party only where the documents are likely to support the case of the applicant or adversely affect the case of one of the other parties to the proceedings, and disclosure is necessary in order to dispose fairly of the claim or to save costs.

Both these applications must be supported by evidence, and the applicant must be able to identify specific documents to which the rule applies, or a class of documents all of which fall within the rule. The orders providing for disclosure may also require the respondent to indicate what has happened to any documents which are no longer in his control, and specify the time and place for disclosure and inspection.

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The CPR contain no express obligation requiring a party to retain documents.

Until litigation is in reasonable contemplation, there is nothing to prevent an organization destroying documents in the normal course of business, subject, of course, to its obligations to retain documents for regulatory or statutory purposes.

However, once an order for disclosure has been made, the party must preserve the documents ordered to be disclosed. It is a contempt of court intentionally to destroy documents which are the subject of a disclosure order (*Alliance & Leicester Building Society v. Gahremani* (1992) 142 N.L.J. 313).

It is not entirely clear whether there is an obligation not to destroy documents which will be the subject of disclosure once proceedings have commenced, but before an order for disclosure has been made. In the Australian decision of *British American Tobacco Australia Services Ltd. v. Cowell* [2002] V.S.C.A. 197, the court thought that there was such an obligation, and that the criterion for the court's intervention by imposing sanctions (not including drawing adverse inferences) is whether the destruction or disposal amounts to an attempt to pervert the course of justice. The court in *Cowell* relied upon the dicta of Megarry J in *Rockwell Machine Tools v. EP Barrus (Commissionaires) Ltd.* [1968] 1W.L.R. 693. *Cowell* was referred to with approval by Morritt V.C in *Douglas -v- Hello (No.3)* [2003] E.W.H.C. 55 (Ch).

However, if there were deliberate destruction of documents after the commencement of proceedings, the court would be unlikely to consider this acceptable. In the case of *Infabrics v. Jaytex* (1986) F.S.R. 75, the court applied the maxim "*omnia praesummuntur contra spoliaterem*"[257] against the defendant who had not preserved documents affecting the quantum of damage and had allowed these to be destroyed after the commencement of the action.

Once litigation is in reasonable contemplation, there is still no express rule which prevents document destruction. However, a deliberate decision to destroy relevant documents when proceedings are imminent, or after their contemplation, could involve a criminal offence of obstructing or perverting the course of justice in some circumstances (*R v. Selvage* [1982] Q.B. 372; *R v. Rowell* (1978) 1W.L.R. 132), and the court may also draw adverse inferences from such an exercise.

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

A deliberate decision to destroy relevant documents when proceedings are imminent or after their contemplation could involve the criminal offence of obstructing or perverting the course of justice in some circumstances (*R. v. Selvage* [1982] Q.B. 372; *R. v. Rowell* [1978] 1W.L.R. 132). The court may also draw adverse inferences from such an exercise.

Where there has been no compliance with an order for disclosure and the lack of disclosure renders it impossible to conduct a fair trial, the court may also consider the remedy of striking out the claim or defence. The criterion for the court's intervention by imposing sanctions (not including drawing of adverse inferences) is whether the destruction or disposal amounts to an attempt to pervert the course of justice: *Douglas v. Hello! Ltd.* [2003] 1 All E.R. 1087.

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

Generally, the court has discretion as to whether costs are payable by one party to another, the amount of those costs and when they are to be paid (CPR 44.3). If the court decides to make an order about costs, the general rule is that the unsuccessful party will be ordered to pay the costs of the successful party, but the court may make a different order (CPR 44.3).

Therefore costs of disclosure are treated in the same manner as all other aspects of litigation: that is to say, there is scope for the successful party to recover its costs of disclosure from the unsuccessful party. However, the court has discretion to depart from this principle if it deems fit. Factors that will affect this discretion include the conduct of all the parties, whether a party has succeeded on part of his case, even if he has not been wholly successful, and also any payment into court or admissible offer to settle made by a party which is drawn to the court's attention (CPR 44.3).

[257] "*Omnia praesummuntur contra spoliaterem*" means "all things presumed against the wrongdoer."

As regards the costs of pre-action disclosure or disclosure from a non-party, there is a specific provision in the CPR which deals with costs in these two areas. The general rule is that the court will award the person against whom the order is sought his costs of the application and of complying with any order made on the application. The court may however make a different order, having regard to all the circumstances, including the extent to which it was reasonable for the person against whom the order was sought to oppose the application and whether the parties to the application have complied with any relevant pre-action protocol (CPR 48.1).

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

Prior to 2004, the CPR were unclear as to how electronic documents were to be dealt with on disclosure. There was also very little guidance from the courts as to whether, and to what extent, the parties should carry out a search for electronic documents, although the courts had made it clear that the meaning of "document" was not restricted to hard copy documents, but extended to anything upon which evidence or information was recorded in a manner intelligible by the use of equipment, *e.g.,* tape recordings (*Grant v Southwestern and County Properties Ltd.* [1974] 2 All E.R. 465). The courts had also ruled that a computer database, which forms part of the business records of a company, insofar as it contained information capable of being retrieved and converted into readable form, is a "document" for the purposes of CPR 31.4 and therefore susceptible to disclosure (*Derby Co. Ltd. v. Weldon (No.9)* [1991] 2 All E.R. 901). The word processing file of a computer was also held to be within the definition of a "document" for the purpose of an order preserving documents in connection with proceedings (*Alliance & Leicester Building Society v. Ghahremani* [1992] R.V.R 198).

The problems relating to electronic disclosure were first highlighted by three members of the Commercial Litigators Forum in a report dated 15 October 2003.[258]

A Commercial Court Working Party on Electronic Disclosure then published a report,[259] in which it recommended that various guidelines be added to the Commercial Court Guide.

The courts responded quickly to the Commercial Court Working Party's report and issued guidelines in the revised Admiralty and Commercial Court Guide dated 26 November 2004. A revised Practice Direction to Part 31 of the CPR dated 1 October 2005, applicable in all the courts, was also approved by the Rules Committee.

The revised Part 31 Practice Direction and Admiralty & Commercial Courts Guide (which are virtually identical) provide a definition of a "document" in the context of electronic documents, provide for the parties to exchange information regarding their searches for and the preservation of electronic documents, and specify the factors the courts will taken into account in deciding what is a "reasonable search" (as required by CPR 3.18).

Since the CPR Part 31 Practice Direction and the Admiralty & Commercial Courts Guide were introduced, there has been very little case law in relation to electronic disclosure.

The first reported case in which the English courts considered this subject was *Hands v. Morrison Construction Services Ltd.* [2006] E.W.H.C. 2018 (Ch). Here the court declined to order pre-action disclosure of electronic documents (despite an offer by the applicant to meet the cost) on the ground that it would be excessively

[258] M. Humphries, N. Mirchandani, S. Bhandari, Electronic Disclosure October 15 2003; "The Future is Electronic," Legal Week, October 30 2003, p. 12.
[259] http://www.hmcourts-service.gov.uk/docs/electronic_disclosure1004.doc.

burdensome (but making a limited order for disclosure of hard copy documents instead). However, the court in that case gave no additional guidance as to how the Practice Direction or the Guide would be applied.

The Court did, however, give guidance as to how Practice Direction 31 would be applied in the case of *Digicel (St. Lucia) Ltd. & Others v. Cable & Wireless Plc & Others* (2008) E.W.H.C. 2522. The Court in that case considered an application by the Claimant for restoration of back-up tapes and for additional search terms against the Defendant. The Defendant had already conducted an extensive search of over 1 million documents at a cost of over £2 million, and claimed that the further searches would be costly and disproportionate. In deciding whether this was a reasonable search, Mr. Justice Morgan did not use as a yardstick the more detailed search conducted by the Claimant, although he said that if the Claimant had done very much less than the Defendant, he might have questioned the application for disclosure.

The Judge did, however, rely on Part 31 Practice Direction and the Commercial Court Working Party Report, and also considered cases decided by the Courts in the US and Australia. Mr. Justice Morgan emphasised paragraph 2A.2 of the Practice Direction, which states that the parties should, at an early stage in the litigation, discuss issues regarding searches for electronic documents, and that key word searches should be agreed between the parties. The Judge held that the Defendant's solicitors' failure to comply with this direction exposed the Defendant to the risk that the Court may order the search to be done a second time.

This failure also led the Judge to order that the parties should first meet and discuss how the back-up tapes should be restored, and he then ordered the Defendant to restore the tapes. He also ordered the Defendant to conduct a further search for electronic documents using some additional search words. Before making this order the Judge considered, in relation to each additional word in the Claimant's application, the proportionality of a further search being carried out and the likelihood of locating further relevant documents by that search.

This case has now made clear to all parties to litigation in England and Wales that they should discuss issues relating to electronic disclosure, and the searches (including key word searches) they intend to carry out, at an early stage in the case.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

In England and Wales, under the CPR, disclosure is limited to "documents" (CPR 31.6). Part 31.4 of the CPR defines "document" as "anything in which information of any description is recorded." The Admiralty & Commercial Courts Guide and the Practice Direction to CPR Part 31 at paragraph 2A.1 have confirmed that a "document" includes "email and other electronic communications, word processed documents and databases." In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been "deleted." It also extends to additional information stored and associated with electronic documents known as "metadata," although paragraph E3.11(a) of the Admiralty & Commercial Courts Guide states that "in most cases metadata is unlikely to be relevant." It would also include electronically recorded communications and activities such as instant messaging on on-line systems (*e.g.,* MSN Messenger) and multimedia files (*e.g.,* voice mail and videos).

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

CPR Practice Direction 31 2A.2 states that the parties should, prior to the first CMC, discuss any issues that may arise regarding searches for and the preservation of electronic documents. This may involve the parties providing information about the categories of electronic documents within their control, the computer systems, electronic devices and media on which any relevant documents may be held, the storage systems maintained by

the parties and their document retention policies. In the case of difficulty or disagreement, the matter should be referred to a judge for directions at the earliest practical date, if possible at the first CMC. The judgment of Mr. Justice Morgan in the *Digicel* case emphasises the importance of complying with this particular provision.

10. *Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.*

CPR Practice Direction 31 makes clear that all electronic documents, wherever they are stored and electronic documents that have been "deleted," may be the subject of disclosure. The general rules and law relating to the preservation and destruction of documents referred to in questions 4 and 5 above also apply in relation to electronic documents.

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

CPR Practice Direction 31 and the revised Admiralty & Commercial Courts Guide give guidance on the scope of the search for electronic documents. They acknowledge the following factors as impacting on the reasonableness of a search for electronic documents:

(a) The number of documents involved.

(b) The nature and complexity of the proceedings.

(c) The ease and expense of retrieval of any particular document. This includes:

(i) The accessibility of electronic documents or data, including e-mail communications on computer systems, servers, back-up systems and other electronic devices or media that may contain such documents taking into account alterations or developments in hardware or software systems used by the disclosing party and/or available to enable access to such documents.

(ii) The location of relevant electronic documents, data, computer systems, servers, back-up systems and other electronic devices or media that may contain such documents.

(iii) The likelihood of locating relevant data.

(iv) The cost of recovering electronic documents.

(v) The cost of disclosing and providing inspection of any relevant electronic documents.

(vi) The likelihood that electronic documents will be materially altered in the course of recovery, disclosure or inspection.

(d) The significance of any document that is likely to be located during the search.

Furthermore, guidance is given that it may be reasonable to search some or all of the parties' electronic storage systems. In some circumstances, it may be reasonable to search for electronic documents by means of keyword searches (agreed as far as possible between the parties), even where a full review of each and every document would be unreasonable.

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

CPR 31.10 states that a party must make a disclosure statement when disclosing documents. This statement should set out the extent of the search that has been made to locate documents which it is required to disclose. Furthermore, the statement should certify that the party understands the duty to disclose documents and that it carried out this duty to the best of its knowledge. In setting out the extent of the search, the party should draw attention to any particular limitations on the extent of the search which were adopted for proportionality reasons, and give the reasons why the limitations were adopted.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

CPR Practice Direction 31 2A.3 states that parties should co-operate at an early stage as to the format in which electronic copy documents are to be provided on inspection. In the case of difficulty or disagreement, the matter should be referred to a judge for directions at the earliest practical date, if possible at the first Case Management Conference.

The format of production is not a problem which should give rise to a dispute, but if it does or the parties need help as to how to produce the documents, The Litigation Support and Technology Group (LiST) has produced a draft Data Exchange Protocol which can be found on its website.[260]

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

The general rules relating to the preservation of documents are referred to in question 4 above; these apply to electronic documents. The legal standard for disclosure is one of reasonableness, as referred to in question 3 above. The rules on production are referred to in question 13 above.

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

CPR 31.20 states that where a party inadvertently allows a privileged document to be inspected, the party who has inspected the document may use it or its contents only with the permission of the court. This rule applies to electronic documents as well as to hard copy documents.

Privileged documents mistakenly disclosed can, however, generally be used by the receiving party on the basis that they are no longer the subject of legal professional privilege where it was not obvious to a reasonable solicitor that a mistake had been made, subject always to the court's powers of case management (see, *Al Fayed and Others v. Commissioner of Police of the Metropolis* [2002] E.C.W.A. Civ. 780).

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

There are no specific rules dealing with costs of electronic disclosure. Costs of this type of disclosure therefore follow the same principles as costs in relation to the rest of the disclosure process as found at CPR Part 44.3 (*see* question 6 above). It is to be remembered that the court has complete discretion as to when and in whose favour costs are to be awarded.

In a case decided under the former Rules of Civil Procedure, *Grupo Torras S.A. v. Al-Sabah* [1998] Masons C.L.R. 90, it was held that where the plaintiffs had scanned 50,000 electronic documents into electronic form

[260] http://www.listgroup.org.

for their own purposes, they could not charge any part of the scanning costs to other parties, but only the costs of producing additional compact discs. The costs of the scanning would form part of the plaintiffs' reasonable costs of the action. The judge said that it was open to a party to seek a direction from court before doing the scanning, and this might include a direction as to the basis for charging for documents produced in electronic form.

The Commercial Court Working Party in its Report dated 6 October 2004 recommended that where substantial costs were incurred in dealing with electronic disclosure, at the conclusion of the trial (or earlier if appropriate), judges should give separate consideration as to the costs incurred and who should pay these costs, having regard to the reasonableness and proportionality of the disclosure requested and given, the relevance of the disclosure given or ordered to be given to the issues in the case presented at trial, and the conduct of the parties generally in relation to disclosure

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

There are literally hundreds of laws that mandate the retention of electronic information for business and legal purposes and the use of information management policies and procedures are required in many situations, including expressly under statute (see, *e.g.,* the Freedom of Information Act 2000), impliedly under statute (see, *e.g.,* the Data Protection Act 1998) and by regulatory guidance (see, *e.g.,* the Financial Services Authority handbook). However, there is no requirement for information management policies and procedures for the purposes of litigation.

The extent to which organizations have adopted information management policies and procedures is unknown.

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The use of electronic information management technologies that assist with the preservation, classification and management of electronic information for legal reasons is widespread. For example, the Freedom of Information Act 2000 has resulted in their widespread adoption within the public sector. "E-discovery" technologies are also being adopted, including by law firms.

Many IT companies can provide compelling evidence of the existence of a "legal compliance driver" within the procurement of IT products and services. For example, data storage vendors have made sales on the back of new rules requiring the retention of communications data by telecommunications companies (see the Communications Data Retention Directive 2006/24/EC).

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

The Human Rights Act 1998 has transposed the European Convention on Human Rights into UK domestic law. Article 8 of the Convention contains the "right to privacy" and for the purposes of domestic law where a person has a "reasonable expectation of privacy" they can sue under the modified law of confidence if they feel that their rights have been infringed. The Data Protection Act 1998 transposes the EC Data Protection Directive into UK domestic law and is intended to ensure a high level of protection for fundamental rights and freedoms, particularly the right to privacy, as well as the maintenance of free flows of personal data around the European Economic Area. The HRA and the DPA can both impact on the disclosure/productions of documents, including electronic documents in legal proceedings and regulatory enquiries.

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

The privacy of electronic data undergoing processing is protected by the Data Protection Act 1998, which transposes the EC Data Protection Directive 95/46/EC, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), which transpose the EC E-Privacy Directive 2002/58/EC. The Human Rights Act 1998 transposes the European Convention on Human Rights into domestic law; Article 8 of the Convention contains the "right to privacy."

The Data Protection Directive is an Internal Market measure, which has two ambitions. First, it seeks to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data. Second, it renders unlawful and restricts prohibitions on the free flow of personal data between countries within the European Economic Area for reasons connected with the protection of the fundamental rights and freedoms. The origins of harmonised EC data protection law can actually be traced back to 1968, when the Council of Europe took its first steps along the legislative path that culminated in the Data Protection Convention 1981.

The Directive contains fours regulatory mechanisms, all of which have been transposed by the Data Protection Act:

a. Transparency mechanisms – Including the obligation to register with the national regulator and the right of subject access.

b. General rules on lawfulness.

c. The right to object – The data subject may object to processing on legitimate grounds, such as where substantial and unwarranted damage or distress is caused.

d. Enforcement mechanisms – The national regulator and the data subject have various rights to enforce the legislative framework.

Most components of the regulatory mechanisms are identified as "data protection principles." There are eight data protection principles within the Data Protection Act, namely:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless —

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The regulatory burdens in the Directive and the Act are born by the "data controller," who has the power to determine both the purpose and manner of processing.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

The Data Protection Act adopts a two stage definition of "personal data", defining first of all the meaning of "data":

"data" means information which —

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68,

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

"Personal data" is defined as follows:

"personal data" means data which relate to a living individual who can be identified —

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

"Sensitive personal data" is defined as follows:

> In this Act "sensitive personal data" means personal data consisting of information as to —
>
> (a) the racial or ethnic origin of the data subject,
>
> (b) his political opinions,
>
> (c) his religious beliefs or other beliefs of a similar nature,
>
> (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
>
> (e) his physical or mental health or condition,
>
> (f) his sexual life,
>
> (g) the commission or alleged commission by him of any offence, or
>
> (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The leading case on the meaning of personal data is *Durant v. Financial Services Authority* (2003), a decision of the Court of Appeal of England and Wales.

"Processing" is defined in the following terms:

> "processing," in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —
>
> (a) organisation, adaptation or alteration of the information or data,
>
> (b) retrieval, consultation or use of the information or data,
>
> (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
>
> (d) alignment, combination, blocking, erasure or destruction of the information or data.

The leading case on the meaning of processing is *Johnson v. Medical Defence Union* (2007), a decision of the Court of Appeal of England and Wales.

c. What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?

Section 35 of the Data Protection Act contains exemptions from the Act's "non-disclosure

provisions" for disclosures required by law or made in connection with legal proceedings. This means that in appropriate cases the data protection principles will not act to prevent disclosures for the purposes of legal proceedings or regulatory enquiries. Section 35 says:

> 35. Disclosures required by law or made in connection with legal proceedings etc.
>
> (1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.
>
> (2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary —
>
> (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
>
> (b) for the purpose of obtaining legal advice,
>
> or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

The Civil Procedures Rules include various provisions against inspection and production of documents. Under CPR 31.3 a litigant giving disclosure is allowed to assert a right or duty to withhold inspection. This right/duty is generally confined to privileged situations. In addition to legal professional privilege and the privilege from self incrimination, documents may be privileged on the grounds that production would be injurious to the public interest. This public interest ground has been held to extend to confidential information that falls within the scope of Article 8 of the European Convention on Human Rights (the right to privacy).

d. Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.

The Human Rights Act and the Data Protection Act both apply to civil and criminal proceedings.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

The beneficiary of the protections contained in the Data Protection Act is the "data subject," who is a natural person; legal persons do not gain protections under the DPA. However, legal persons do enjoy the protections of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended). Legal persons do enjoy the protection of the Human Rights Act, but the extent to which the right to privacy extends to legal persons has yet to be conclusively determined.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

The Data Protection Act contains many exemptions, most of which are contained in Part IV of the Act. Article 8(2) of the European Convention on Human Rights contains the substantial "carve out" from the right to privacy; interferences with privacy will be lawful where they are in accordance with law, necessary in a democratic society and for legitimate purposes. The DPA reflects this.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

There are no specific data types, subject areas or situations for which electronic discovery is restricted. Disclosure of documents in litigation must be conducted in accordance with the Civil Procedures Rules and the main ground for withholding inspection is privilege.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

The immediate answer is repeated.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

The Information Commissioner is the UK regulator under the Data Protection Act. Most data controllers are required to register within the Commissioner prior to the commencement of processing, although there are exemptions from this rule. In addition, in order to satisfy the first data protection principle, which requires processing to be fair and lawful, data controllers have to notify data subjects of their identity and intentions, but, again, there are exemptions.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

A litigant wishing to compel the disclosure of documents containing personal data must follow the procedures contained in the Civil Procedure Rules. However, a data controller is entitled to disclose personal data on a voluntary basis under section 35 of the Data Protection Act, if satisfied that the disclosure is "necessary" for defined legal purposes. The Information Commissioner can obtain personal data by serving a data controller with an "information notice" under section 43 of the DPA.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

In order to satisfy the first data protection principle (fair and lawful processing) the data controller must be able to demonstrate the existence of a criterion for legitimate processing. Consent is one such criterion and in an employment situation consent will often be the criterion of choice.

Likewise, consent provides a valid ground for the transfer of data from the European Economic Area to a country that does not provide an adequate level of protection for personal data.

Employers wishing to rely upon employee consent to legitimize processing and transfers of data must be cautious however; consent must be "freely given" and it is arguable that in some situations the employee's consent might not be such.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

The United Kingdom is a party to The Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters. The UK is also subject to the Taking of Evidence Regulation (Council Regulation 1206/2001). There is no blocking statute in the UK.

Where the request for documentation comes from a State that is not subject to Regulation 1206/2001, but is a party to The Hague Convention the request is considered under the Evidence (Proceedings in Other Jurisdictions) Act 1975 and CPR 34.16 to 34.21. Section 2 of the Act says:

> 2.—Power of United Kingdom court to give effect to application for assistance.
>
> (1) Subject to the provisions of this section, the High Court, the Court of Session and the High Court of Justice in Northern Ireland shall each have power, on any such application as is mentioned in section 1 above, by order to make such provision for obtaining evidence in the part of the United Kingdom in which it exercises jurisdiction as may appear to the court to be appropriate for the purpose of giving effect to the request in pursuance of which the application is made; and any such order may require a person specified therein to take such steps as the court may consider appropriate for that purpose.
>
> (2) Without prejudice to the generality of subsection (1) above but subject to the provisions of this section, an order under this section may, in particular, make provision —
>
> (a) for the examination of witnesses, either orally or in writing;
>
> (b) for the production of documents;
>
> (c) for the inspection, photographing, preservation, custody or detention of any property;
>
> (d) for the taking of samples of any property and the carrying out of any experiments on or with any property;
>
> (e) for the medical examination of any person;
>
> (f) without prejudice to paragraph (e) above, for the taking and testing of samples of blood from any person.
>
> (3) An order under this section shall not require any particular steps to be taken unless they are steps which can be required to be taken by way of obtaining evidence for the purposes of civil proceedings in the court making the order (whether or not proceedings of the same description as those to which the application for the order relates); but this subsection shall not preclude the making of an order requiring a person to give testimony (either orally or in writing) otherwise than on oath where this is asked for by the requesting court.

> (4) An order under this section shall not require a person —
>
> (a) to state what documents relevant to the proceedings to which the application for the order relates are or have been in his possession, custody or power; or
>
> (b) to produce any documents other than particular documents specified in the order as being documents appearing to the court making the order to be, or to be likely to be, in his possession, custody or power.
>
> (5) A person who, by virtue of an order under this section, is required to attend at any place shall be entitled to the like conduct money and payment for expenses and loss of time as on attendance as a witness in civil proceedings before the court making the order.

CPR 34.17 provides that applications under the 1975 Act must be made to the High Court, they must be supported by written evidence and they must be accompanied by the request as a result of which the application is made and, where appropriate, a translation into English. Applications can be made without notice. An order for disclosure will only be made where proceedings have been commenced in the foreign court, or are pending, and in a case where documents are sought an order will only be made in respect of particular, specified documents and then only to the extent that they would be disclosable in litigation in the jurisdiction; an order equivalent to standard disclosure under CPR 31 will not be made and documents will not be disclosable where a claim to privilege is made out.

Where the request comes from a State that is subject to Regulation 1206/2001 (the EU, bar Denmark) the request is dealt within under CPR 34.24. Initial points to note are:

1. The request must be made by a court of another Regulation State.
2. The request must be made to the designated court, either in English or in French (translations should be supplied as appropriate).
3. The request must be accompanied by a "form of request."

Upon receipt of the request it is sent by the court to the Treasury Solicitor, who may then make an application for "evidence to be taken." If the court approves the application the Treasury Solicitor will make the necessary arrangements for the taking of evidence. This will lead to the taking of a deposition, which, ultimately, will be sent to the requesting party. The usual rules on privilege will apply.

United States

William Butterfield - ***Lead Editor***
Steve Bennett, Regan Adams, Conor Crowley, Wayne Matus, Paul Robertson - ***Contributing Editors***
David Kessler, Annie Goranson - ***Second Reader***

The Law Relating to Discovery/Disclosure in General

1. *Please describe your civil litigation system, specifying whether it is a common law or civil code jurisdiction, whether it is a multi-tiered judicial system, such as the federal/local systems in the United States and Australia, and how the law relating to document disclosure is developed, e.g., by case law or rules. The Commonwealth of Australia, a federation of six states and a number of territories (3 of which are self-governing), is a common law jurisdiction and has a multi-tiered judicial system at both the federal and state levels.*

   The United States is a common law jurisdiction at the national level. There are separate government and court systems within each of the 50 states. With one exception (Louisiana), the individual states also follow the common-law tradition.

   In the national or "Federal" courts, discovery is governed by the Federal Rules of Civil Procedure (the "Fed R. Civ. P."). Each of the 50 states has its own set of rules that are similar, and in some cases identical to, the Fed. R. Civ. P. These rules are frequently interpreted by trial courts during pre-trial rulings, and these rulings are published as official interpretations of the relevant rules. Practitioners rely upon what has become an enormous body of case law, as well as official commentary to the rules, to interpret the meaning of the relevant rules.

   In December 2006, after several years of discussion, commentary, and public discussion, the Federal Rules were amended to add additional and changed language to address perceived problems caused by the impact that the discovery of electronically stored information ("ESI") has had on the discovery process. The amendments were proposed by the U.S. Supreme Court and adopted into law with the acquiescence of the U.S. Congress. These new rules are discussed in more detail below. At least one state, New Jersey, has adopted the amendments, and many other states have adopted amendments modeled on the Federal Rules.[261]

2. *Please specify what obligations a party to civil court proceedings in this jurisdiction has to disclose documents, including a discussion of the scope of this obligation. Describe the stage in the proceedings when such disclosure takes place, specifying whether this is an automatic obligation or one that has to be requested or ordered. For this and each following question, please describe and provide a copy of any applicable statutory provisions or rules.*

   U.S. discovery is widely considered to be the broadest and most permissive in the world.[262] Although parties are obligated to engage in a limited amount of self-initiated disclosure (called "initial disclosures") at the outset of the case, the vast majority of document discovery takes place through a series of requests and productions exchanged between the parties.

   These discovery obligations and privileges are governed by Fed. R. Civ. P. 26 and 34. Fed. R. Civ. P. Rule 26(a)(1) obligates parties to disclose at the outset of the case, without awaiting a discovery request, "a copy, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." As a practical matter, most parties do not engage in any meaningful

[261] Because a fifty-state survey would not be useful for the purposes of this comparative analysis, this section on U.S. law will address the law at the Federal level only. It should be noted however, that the various jurisdictions are more alike than not, especially when contrasted with the law existing outside of the United States.

[262] *See, e.g.,* Stephen N. Surbrin, *Discovery in a Global Perspective: Are We Nuts,* 52 DePaul L. Rev. 299, 301-14 (2002) (discussing a variety of factors relating the expansive nature of discovery in the United States in comparison with other countries); Geoffrey G. Hazard, Jr., *From Whom No Secrets Are Held*, 76 Tex. L. Rev. 1665, 1673 (1998) ("Put bluntly, the impression of American discovery in most foreign countries is that of an alien legal regime conducting a warrantless search in someone else's domestic territory").

exchange of document discovery at this stage of the proceedings, both because one need disclose only favorable documents, and because the obligation can be met by describing the documents without producing them.

It is through Fed. R. Civ. P. Rule 34 that meaningful document discovery takes place. Fed. R. Civ. P. Rule 34(a) provides that:

> [a]ny party may serve on any other party a request (1) to produce and permit the party making the request . . . to inspect, copy, test, or sample any designated documents or electronically stored information [that] constitute or contain matters within the scope of Fed. R. Civ. P. Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served . . . ."

With respect to scope, Fed. R. Civ. P. 26(b)(1) states that "[p]arties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party . . . ." As articulated by the Supreme Court, broad discovery rights in the U.S. system are aimed at reducing the possibility of unfair surprise at trial.

Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. To that end, either party may compel the other to disgorge whatever facts he has in his possession. The deposition-discovery procedure simply advances the stage at which the disclosure can be compelled from the time of trial to the period preceding it, thus reducing the possibility of surprise.[263] Thus, parties are permitted to discover not only admissible facts, but also information that appears "reasonably calculated to lead to the discovery of admissible evidence" (Fed. R. Civ. P. 26(b)(1)).

Document discovery is not completely without limit. Permissible scope is constrained by whether "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues" (Fed. R. Civ. P. 26(b)(2)). The states generally mimic the liberal discovery principles that exist in the Federal Courts.

3. *Is there a right to obtain pre-action disclosure or disclosure during the proceedings from a non party? If so, please describe the circumstances in which these rights arise and the nature of the obligation to give disclosure.*

As a general matter, pre-action discovery is unavailable to private parties under Federal law within the United States. There are certain narrow exceptions, the most notable being where "there is a 'significant risk' that the evidence will be lost if it is not perpetuated."[264] The circumstances in which such evidence can be collected are narrowly constrained, including a general prohibition against using Fed. R. Civ. P. Rule 27 as a tool for collecting discovery to determine if a cause of action exists.[265] Although Fed. R. Civ. P. Rule 27 is geared primarily to address preserving evidence through the taking of a deposition, document discovery is also contemplated.

One should also keep in mind, however, that under U.S. law one can file a claim first, and collect the evidentiary support for it later through discovery, as long as one has a good faith belief that one will be able to do so.[266] The concept of "notice" pleading permits parties to set forth a mere outline of the factual and legal case, as long as the relevant elements for each of the claims are addressed.[267]

---

[263] *Hickman v. Taylor*, 329 U.S. 495, 507, 67 S.Ct. 385, 392 (1947).

[264] *See Tennison v. Henry*, 203 F.R.D. 435, 440 (N.D. Cal. 2001).

[265] *See, e.g., In re Boland*, 79 F.R.D. 665, 668 (D.D.C. 1978 (Rule 27(a) "is not a method of discovery to determine whether a cause of action exists") (internal citation omitted); 4 Moore's Federal Practice ¶ 27.07[4], at p. 27-29 (1989) (where there is no showing of a substantial danger of loss of the evidence, "a person cannot take advantage of Rule 27 merely for the purpose of obtaining facts on which to base a complaint.").

[266] *See* Fed. R. Civ. P. 11(b) (By presenting a pleading to the court, the submitting party or attorney "is certifying that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances, . . . (3) the allegations and other factual contentions have evidentiary support, or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery . . . .").

[267] *See* Fed. R. Civ. P. 8(a) (a pleading that "sets forth a claim for relief . . . shall contain . . . (2) a short and plain statement of the claim showing that the pleader is entitled to relief.").

Once an action has been commenced, the Rules permit the discovery of documents from third parties through the service of a subpoena under Fed. R. Civ. P. Rule 45.

While the Federal Rules permit issuance of a subpoena for documents only, without also requiring a witness to appear for testimony, many state courts do not, and permit requests for documents only in conjunction with a deposition. In general, the scope of discovery permissible with respect to third parties is narrower than with respect to parties to the case.[268]

Most states follow the federal example and do not permit pre-action discovery; however, there are exceptions.[269]

4. *Please describe any obligation a party, or potential party, has to preserve documents for the purpose of civil proceedings, and when that obligation arises.*

The duty to preserve documents has become a principle part of U.S. litigation, with a number of high-profile multi-million – and even multi-billion dollar – cases turning, in large part, on a party's failure to preserve documents. For example, a Florida jury awarded more than $1.4 billion in damages to plaintiff investor Ronald Perelman after the Florida state court took the unusual step of shifting the burden of proof to defendant financial services firm Morgan Stanley after finding that it had failed to preserve and produce relevant emails.[270]

Under U.S. law, the obligation to preserve evidence arises "when the party has notice that the evidence is relevant to the litigation or when a party should have known that the evidence may be relevant to a future litigation."[271]

Although it is generally true that a vague rumor or frivolous threat does not trigger a preservation duty, the obligation to preserve can also arise absent the threat of a specific, predictable, and identifiable litigation. Although the law is not uniform with respect to this duty, some generalities can be observed. For example, courts have imposed sanctions on parties for destroying documents prior to the time that the statute of limitations had expired related to potential claims to which the documents relate.[272] Courts have also held, however, that there must be some "temporal proximity" between the time of the supposed spoliation and the "foreseeability of the harm to the non-spoliating litigant . . . ."[273] Where relevant documents are destroyed prior to litigation pursuant to a records management policy, courts have also considered the destroying party's "good faith" in creating and applying the policy.[274]

With respect to the scope of this preservation duty, it is in alignment with, although somewhat broader than, the duty to produce documents discussed above.

---

[268] *See* Fed. R. Civ. P. 45(c)(1) ("A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena."); *see also Theofel v. Farey Jones*, 341 F.3d 978 (9th Cir. 2003), *amended by* 359 F.3d 1066 (9th Cir. 2004) (court sanctioned party for serving overbroad subpoena for email messages kept by third party Internet Service Provider).

[269] *See, e.g., McNeil v. Jordan*, 586 Pa. 413 (2006)).

[270] *See Coleman Holdings v. Morgan Stanley*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005); *see also Jill Barton,* Perelman Wins $1.4 Billion Total in Suit Against Morgan Stanley, The Associated Press, May 19, 2005, *available at* http://www.law.com/jsp/article.jsp?id=1116407110202.

[271] *See Fujitsu Ltd. v. Federal Express Corp.,* 247 F.3d 423, 436 (2d Cir. 2001); *see generally Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) ("*Zubulake IV*") (currently considered the touchstone case with respect to the duty to preserve). Many organizations are also subject to a variety of statutory and regulatory requirements that require particular documents, including electronic documents, to be retained for specified periods of time. *See, e.g.*, Sarbanes-Oxley Act of 2002, 116 Stat. 745 (2002) (enacted in response to recent wave of corporate scandals and charges of accounting irregularities and contains a number of document retention requirements applicable to publicly traded companies); 17 C.F.R. § 240.17a-4(b)(4) (promulgated by the Securities and Exchange Commission pursuant to the Securities Exchange Act of 1934 and requires retention for three years of "originals of all communications received and copies of all communications sent by [each] member, broker, dealer (including inter-office memoranda and communications) relating to his business as such"). The regulatory obligation to preserve is sometimes relevant to the obligation to preserve in the civil litigation setting. *Compare Byrnie v. Town of Cromwell Bd. of Education*, 243 F.3d, 93, 108-09 (2nd Cir. 2001) (discussing instances were courts have held that "destruction of evidence in violation with a regulation that requires its retention can give rise to an inference of spoliation.") *with Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 322 n.70 (S.D.N.Y. 2003) ("*Zubulake I*") (holding that plaintiff is not an intended beneficiary of the preservation regulation at issue).

[272] *See Reingold v. Wet'N Wild Nevada, Inc.*, 944 P.2d 800, 802 (Nev. 1997) (adverse inference instruction appropriate where defendant amusement park's document retention policy resulted in the routine destruction of first aid logs at the end of each season, long before the subject complaint was filed, but also before the statute of limitations had run on potential claims).

[273] *See Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892 (Cal. Ct. App. 1995) (court finds no spoliation where tractor manufacturer destroyed the relevant documents ten years before the plaintiff was injured, the documents had not been previously routinely requested, and where the "evidence disclosed only one other accident involving [the general nature of the alleged failure] and none involving [the particular alleged failure at issue].").

[274] *See, e.g., Stevenson v. Union Pacific*, 354 F.3d 739, 747 (8th Cir. 2004) ("Where a routine document retention policy has been followed in this context, we now clarify that there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction.").

> While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, [or] is reasonably likely to be requested during discovery . . . .[275]

5. *Please specify what penalties or sanctions can be imposed on a party for failure to preserve documents for the purposes of litigation, and in what circumstances these penalties or sanctions are imposed.*

A party that fails to meet the preservation obligations set forth above can be subject to a broad array of sanctions ranging from a mere stay of discovery or trial to the entry of an adverse judgment. A court derives the power to sanction a party for failing to preserve documents from the civil rules,[276] from the court's inherent power to manage its affairs,[277] and from a common law duty to preserve evidence for trial.[278]

Sanctions for evidence spoliation serve many purposes. As described in *United Medical Supply Co. Inc. v. United States*, 77 Fed. Cl. 257 (Fed. Cl. June 27, 2007), they serve to punish the spoliator and thereby ensure that it does not benefit from its misconduct; to deter future misconduct; to remedy or minimize the financial impact caused by the spoliation; and to preserve the integrity of the judicial process and its truth-seeking function.[279]

The federal circuit courts are split on whether it is necessary to show bad faith on the part of the spoliator before imposing sanctions. Some circuits require a showing of bad faith before any form of sanction is imposed. Some allow for spoliation sanctions on a mere showing of negligence. Still others require something more than negligence, requiring a showing of purposeful, willful or intentional conduct.[280]

In general, the more egregious the offending party's conduct and the greater the prejudice caused, the more punitive the sanction is likely to be.[281]

A trial court has a broad array of sanctions available to enable it to fashion the appropriate penalty.[282] The sanctions available to the court include: (1) delaying discovery or trial;[283] (2) requiring the offending party to pay the costs and fees incurred by the requesting party related to the offending conduct;[284] (3) refusing to allow the offending party to adduce certain facts or put on certain witnesses related to the offending conduct;[285] (4) reading an adverse inference instruction to the jury;[286] (5) shifting the burden of proof to the offending party;[287] (6) treating matters or facts related to the offending conduct as admitted for the purposes of the action;[288] (7) declaring a mistrial;[289] (8) striking pleadings (see Fed. R. Civ. P. 37(b)(2)(C)); or (9) entering a default judgment

---

[275] *Zubulake IV*, at 218 (quoting *William T. Thompson Co. v. General Nutrition Corp.,* 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)).

[276] *See* Fed. R. Civ. P. 37(b)(2) (setting forth an array of sanctions that may be entered against a party that fails to comply with a discovery order). Additional sanctioning authority is provided under Fed. R. Civ. P. 11, 26(e) and 26(g).

[277] *See Residential Funding Corp. v. DeGeorge Fin. Corp.,* 306 F.3d 99, 106-07 (2d Cir. 2002) ("Even in the absence of a discovery order, a court may impose sanctions on a party for misconduct in discovery under its inherent power to manage its own affairs."); *see also Zubulake IV*, at 212.

[278] *See, e.g., Silvestri v. General Motors,* 271 F.3d 583 (4th Cir. 2001) (addressing the "common law of spoliation").

[279] *See also Nat'l Hockey League v. Metro Hockey Club, Inc.*, 427 U.S. 639, 642-43, 96 S.Ct. 2778, 49 L.Ed.2d 747 (1976).

[280] For a thorough discussion and comparison of the cases on this issue, *see generally United Med. Supply Co. Inc., v. United States*, 77 Fed. Cl. 257, 266-67 (Fed. Cl. June 27, 2007).

[281] *See, e.g., New York State Nat'l Org. for Women v. Cuomo*, 1998 WL 395320, *2-3 (S.D.N.Y. July 14, 1998) (rejecting request for sanctions against defendant for destroying computer databases because there was little evidence of bad faith and plaintiffs were not prejudiced by the loss); Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 Mich. Telecomm. Tech. L. Rev. 71, 80 (2004) ("the results of [a survey conducted by Judge Scheindlin and her clerk] reveal that the profile of a typical sanctioned party is a defendant that destroys electronic information in violation of a court order, in a manner that is willful or in bad faith, or causes prejudice to the opposing party.").

[282] S*ee Reilly v. Natwest Markets Group, Inc.,* 181 F.3d 253, 267 (2d Cir. 1999) ("Whether exercising its inherent power, or acting pursuant to Rue 37, a district court has wide discretion in sanctioning a party for discovery abuse.").

[283] *See* Fed. R. Civ. P. 37(b)(2)(C); *see also Pennar Software Corp. v. Fortune 500 Sys. Ltd*., 2001 WL 1319162 (N.D. Cal. Oct. 25, 2001) (court sanctioned defendant for electronic discovery abuses by extending discovery period and requiring payment of attorney's fees).

[284] *See* Fed. R. Civ. P. 37(b)(2)(C); *see also Linnen,* 1999 WL 462015 (Mass. Super. June 16, 1999).

[285] *See* Fed. R. Civ. P. 37(b)(2)(B), *see also United States v. Philip Morris USA, Inc.,* No. Civ. 99-2496, 2004 WL 1627252 (D.D.C. July 21, 2004) (where defendants continued to delete relevant email for two years after court ordered preservation, court precluded defendants from calling a key employee and ordered defendants to pay costs relating to the spoliation and an additional $2,750,000 monetary sanction); *United Medical Supply Co. Inc. v. United States*, 77 Fed. Cl. 257 (Fed. Cl. June 27, 2007) (limiting use of expert witnesses to fill in gaps in evidence created by the spoliation).

[286] *See, e.g., Anderson v. Crossroads Capital Ptrs., L.L.C.*, No. Civ. 01-2000, 2004 WL 256512 (D. Minn. Feb. 10, 2004).

[287] *See Coleman Holdings v. Morgan Stanley*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (court shifts to defendant Morgan Stanley burden of showing that it was not guilty of conspiring to defraud plaintiff, after finding that Morgan Stanley had wrongfully overwritten backup tapes containing only copy of relevant emails).

[288] *See* Fed. R. Civ. P. 37(b)(2)(A).

[289] *See Residential Funding Corp.,* 306 F.3d at 107).

against, or dismissing the claims of, the offending party (see Fed. R. Civ. P. 37(b)(2)(C)).[290] Finally, courts sometimes devise creative sanctions in attempting to fashion the appropriate remedy for spoliation. For example, in *Treppel v. Biovail*, 2008 WL 866594 (S.D.N.Y. April 2, 2008), the court found that a party failed to preserve evidence but declined to issue an adverse inference because the requesting party could not show that the lost evidence would have supported his claims. Instead, the court allowed the requesting party to conduct a forensic search of the CEO's hard drive.

In general, a court will enter judgment as a sanction only when the offending conduct is particularly egregious and the destroyed evidence particularly prejudicial. Unless both of these factors are present, courts will typically consider less drastic sanctions.[291]

In situations where a default judgment might be considered too harsh a sanction, courts may instead consider reading an adverse inference instruction to the jury, thereby allowing the jury to infer that the spoliated evidence would have been unfavorable to the party responsible for its destruction had it not been destroyed.[292]

In general, a court will order such an instruction where it finds that: (1) evidence was destroyed; (2) at a time when there was a duty to preserve; (3) with a "culpable" state of mind (meaning with conduct that rises to the level of negligence, gross negligence, or recklessness); which (4) prejudiced the requesting party because the evidence would have supported the requesting party's case or would otherwise have been of a nature alleged by the requesting party. For some courts, in those situations where the offending party's conduct rises to the level of bad faith or willfulness, the requesting party need not adduce separate evidence of prejudice, as the bad faith behavior will be treated as sufficient circumstantial evidence that the destroyed documents would have been harmful to the offending party.[293]

6. *Please describe how the costs of discovery/disclosure are dealt with in civil proceedings.*

As a general rule, the US is not a "loser pays" jurisdiction, and, absent certain fee shifting exceptions, each party bears its own litigation costs, including costs related to the production of documents.[294] This theme was echoed in a number of early cases discussing costs related to producing electronically stored information.[295]

The primary exception to this general rule derives from the dictates of Federal Rule 26(c), which protects parties against unduly burdensome discovery. That Rule provides, in pertinent part, as follows:

> The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of

---

[290] While these cases concern sanctions in civil suits, a party should also be cognizant of the possibility that criminal prosecution can result under obstruction of justice charges when relevant and discoverable documents are destroyed. *See United States v. Lundwall*, 1 F. Supp. 2d 249, 250 (S.D.N.Y. 1998) (holding that defendants who allegedly withheld and destroyed documents sought during the discovery of a civil action could be prosecuted for such conduct under the obstruction of justice statute, 18 U.S.C. § 1503); *see also* Sarbanes-Oxley Act of 2002, 116 Stat. 745 (2002).

[291] *See, e.g., Rice v. City of Chicago*, 333 F.3d 780 (7th Cir. 2003) ("[I]t is well settled in this circuit that the ultimate sanction of dismissal should be invoked only in extreme situations when there is a clear record of delay or contumacious conduct, or when other less drastic sanctions have proven unavailable."); *Wiginton v. Ellis*, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) ("A default judgment, or conversely, dismissal of an action, are harsh sanctions that should only be employed in extreme situations . . . .") (internal quotations removed).

[292] *See Anderson*, 2004 WL 256512 at *2, 8 (where plaintiff used a data purging software application after plaintiff agreed not to "delete any existing files," court found that plaintiff's "exceedingly tedious and disingenuous claim of naiveté" defied "the bounds of reason," but was sufficient only to warrant an adverse inference jury instruction and not dismissal of the case).

[293] S*ee Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 at *27-28 (S.D.N.Y. 2004) ("*Zubulake V*") (court discusses standard for permitting adverse inference); *Wiginton v. Ellis*, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) (in determining whether to draw an inference that destroyed documents would have favored plaintiffs, court must look at facts surrounding the destruction for whether the destruction shows bad faith.); *Residential Funding*, 306 F.3d at 108 ("The inference is adverse to the destroyer not because of any finding of moral culpability, but because the risk that the evidence would have been detrimental rather than favorable should fall on the party responsible for its loss.").

[294] *See, e.g., Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978) ("[T]he presumption is that the responding party must bear the expense of complying with discovery requests . . . .").

[295] *See, e.g., In re Brand Name Prescription Drugs*, 1995 WL 360526 at *2 (Because the producing party chose the electronic storage method at issue, "the necessity of a retrieval program or method is an ordinary and foreseeable risk").

> the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

Thus, a responding party may invoke the court's Rule 26(c) discretion to grant orders providing protection from "undue burden or expense," including orders conditioning discovery on the requesting party's paying discovery costs. As is discussed in more detail below, the practical application of this rule in the context of electronic discovery has been refined in a series of cases addressing the topic.[296]

E-Discovery/E-Disclosure

7. *As a general matter, please describe whether case law or specific rules have developed relating to electronic disclosure. Only a high-level description of the playing field is sought, and details regarding the specific application of the relevant rules and laws may be provided in response to the more targeted questions below.*

In the US, the development of law to address the unique features of electronic discovery has roughly mirrored the progress of the information revolution itself. Although the Rules have moved more slowly than the case law, the end result is the development of a robust body of rules and cases addressing many aspects of ESI disclosure. Recent amendments to the Rules have brought sweeping changes to the landscape, and courts, practitioners, and clients are working now to adapt to these new Rules.

As was discussed above, the discovery of documents is addressed by Federal Rule of Civil Procedure 34. In 1970, at the advent of the information revolution, Rule 34 was amended in "accord with changing technology" to include the phrase "data compilations" under the definition of document to make it clear that "Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices . . . ."[297] Applicable case law has followed suit.[298]

The determination that ESI is discoverable does not, of course, address a myriad of other issues that often arise when discovery involves ESI. As is discussed below, case law has developed to address most of the ancillary issues that have surfaced relating to the disclosure of ESI, and there are literally thousands of cases that discuss the discovery of electronically stored information in state and federal courts. Those cases are publicly available and most can be relied upon for purposes of precedent.[299]

Sometimes, the rules and cases that were developed to address paper discovery have provided a sufficient platform from which to develop approaches to these unique problems, but they have other times been found wanting.[300] As a result, some pressure had grown over the last several years to amend the Federal Rules to address with more clarity certain aspects of ESI disclosure. In 2004, after an exhaustive process of studies and conferences, the Advisory Committee on the Federal Rules of Civil Procedure promulgated proposed revisions to the Federal Rules. The proposed e-discovery rules were modified by the Advisory Committee in April 2005 to address public comments. The revised proposed rules were approved by the Judicial Conference of the United States in late 2005 and by the United States Supreme Court on April 12, 2006. The Rules were adopted and became law on December 1, 2006.

---

[296] *See Zubulake I,* at 309 and *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("*Zubulake III*").

[297] *See* Notes of Advisory Committee on 1970 Amendments to Rules; *see also* A C. Wright, A. Miller & R. Marcus, Federal Practice and Procedure § 2218 at 450 (1994) (1970 amendment of Rule 34 "brought the federal rules . . . into the computer age").

[298] *See, e.g., Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94CIV.2120, 1995 WL 649934 at *2 (S.D.N.Y. Nov. 3 1995) (observing that "it is black letter law that computerized data is discoverable if relevant").

[299] A number of websites offer free links to, copies of and discussion of cases specifically relating to electronically stored information. *See, e.g.,* K&L Gates Electronic Discovery Law, http://www.ediscoverylaw.com; Kroll OnTrack, http://www.krollontrack.com.

[300] For good discussions of the new challenges posed by the disclosure of ESI and the sufficiency of pre-amendment Rules and case law to address them, *see* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 346 (2000) (noting that the Federal Rules have historically provided only "limited guidance" regarding the details of electronic discovery) and *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* (Sedona Conference Working Group Series 2004). http://www.thesedonaconference.org. (discussing which aspects of ESI unique issues can be addressed by extant case law and rules).

The revised Rules address several issues specifically relating to e-discovery, including a definition of "electronic documents," the form of production of electronically stored information, the "accessible" nature of certain forms of e-discovery, and preservation of privilege in the course of e-discovery projects. These rules will retroactively affect cases in federal court and pending cases in federal court "insofar as just and practicable." U.S. Supreme Court Order 2006-15 (April 12, 2006). The U.S. is thus operating under a relatively new regime with respect to e-discovery law. While the general consensus is that the new rules have greatly altered the landscape, the details of that alteration remain to be seen.

8. *Please describe any legal provisions or rules (in place or proposed) that specify how an "electronic document" or "electronic data" is defined for disclosure purposes.*

Since a 1970 amendment, Rule 34 of the Federal Rules of Civil Procedure has included "data compilations" among the "documents and things" that may be subject to production and inspection in discovery.[301]

As noted above, the term "document" has long been understood to encompass "electronic documents."[302] The 2006 Amendments added a description of electronically stored information ("ESI") to include, among other things, "sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained" (Fed. R. Civ. P. 34(a)(1) (2006)). The Advisory Committee noted that this change was to make clear that "discovery of electronically stored information stands on equal footing with discovery of paper documents" (Fed. R. Civ. P. 34(a), 2006 Advisory Committee Note). This "equal footing" is carried through the 2006 Amendments, with several areas where additional or separate provisions are made for dealing with the unique issues of e-discovery. Due to the ever changing nature of technology, the term "electronically stored information" was left vague including information "stored in any medium" to encompass technologies not yet contemplated.[303]

9. *Please describe any legal provisions or rules (in place or proposed) that require the parties to meet and discuss electronic disclosure.*

The 2006 Amendments establish specific requirements regarding parties' obligations to meet and confer and to disclose information about ESI early in the litigation process. There are three main areas for such disclosure and discussion.

First, Rule 26 has long required parties to make initial disclosures regarding evidence and potential witnesses before being served with discovery. Parties were required to disclose copies or descriptions of anything in the party's possession or control that it might use to support its claims or defenses. The 2006 Amendment specifically includes ESI as part of this initial disclosure. This means that very early in the litigation, each party must be able to identify and describe "by category and location" ESI that it intends to use in the litigation (Fed. R. Civ. P. 26(a)(1)(b)).

Second, Rule 26 also requires the parties to "meet and confer" early in the litigation process to discuss, among other things, a discovery plan for the litigation. The 2006 Amendments added to those obligations a requirement that the parties discuss issues related to the preservation and disclosure of ESI, including the form in which ESI is to be produced (Fed. R. Civ. P. 26(f)).

Third, Rule 16, which governs initial scheduling orders, now provides that the court's scheduling order *may* include "provisions for disclosure or discovery of" ESI, as well as discussions of any privilege issues.

---

[301] *See* 1970 Advisory Committee Notes ("The inclusive description of 'documents' is revised to accord with changing technology").

[302] *See Bills v. Kennecott Corp.*, 108 F.R.D. 459, 461 (D. Utah 1985) ("It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the Rules.").

[303] Committee Notes to Fed. R. Civ. P. Rule 34(a)(1); *see Columbia Pictures v. Bunnell,* 2007 U.S. Dist. LEXIS 46364, *24 (C.D. Ca. June 19, 2007)("Based on the evidence in the record, the court finds that the Server Log Data in this case is transmitted through and temporarily stored in RAM while the requests of defendants' website users for dot-torrent files are processed. Consequently, such data is electronically stored information under Rule 34.").

10. Please describe any legal provisions or rules (in place or proposed) that require a party to preserve electronic documents related to pending or possible future litigation.

The obligation to preserve documents, and the sanctions that can result for failure to do so, are discussed above. Specifics relating to electronic documents are discussed here.

According to the leading case in the area of preservation,[304] with the obligation to preserve electronic documents have come a series of subsidiary obligations for parties and their counsel related to locating and preserving ESI.[305] These include counsel's obligation to:

a. Become "fully familiar" with the client's "data retention architecture" and "document retention policies." This entails speaking with information technology personnel "who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy."[306]

b. Interview each of the "key players" to understand how they stored information and communicate the preservation obligation to them in clear terms.[307]

c. Take "reasonable steps" to ensure that the client actually complies with the litigation hold, including periodically reissuing the litigation hold so that it is "fresh in the minds of all employees." It is "not sufficient to notify all employees . . . and expect that the party will then retain and produce all relevant information." A party "cannot reasonably be trusted to receive the 'litigation hold' instruction once and to fully comply with it without the active support of counsel."[308] [309]

As discussed above, some of the country's biggest cases have turned on the alleged failure to preserve electronic documents. Corporate America had lobbied for a change in the Rules that would provide them with a so-called "safe harbor," giving them some protection against excessively punitive sanctions when the failure to retain ESI related to automated systems operating in the absence of bad faith. The 2006 Amendments did, in fact, include language on this topic, but some critics contend that it does not provide the "safe harbor" that had been sought.[310]

Amended Rule 37(e) states that, "Absent exceptional circumstances, a court may not impose sanctions under these 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."[311] Notably, the protections afforded by Rule 37(e) are limited by the language of the Rule itself. Among other things, the Rule does not define "exceptional circumstances," "routine operation," "good faith operation" or "electronic information system." Whether a party is protected from sanctions under Rule 37(e) ultimately depends on the court's interpretation of these terms in each particular case.

---

[304] The leading case, *Zubulake*, is actually a series of five rulings handed down over many months related to the same case but which addresses nearly the full gamut of issues that arise relating to e-disclosure disputes.

[305] *See Zubulake V*.

[306] *Id.* at 432.

[307] *Id.* at 433-34.

[308] *Id.* at 432.

[309] *Id.* However, "[O]f course, it is true that counsel need not supervise every step of the document production process and may rely on their clients in some respects . . ." (at 435), and "[a]t the end of the day …the duty to preserve and produce documents rests on the party. Once that duty is made clear to a party, either by court order or by instructions from counsel, that party is on notice of its obligations and acts at its own peril"(at 436).

[310] *See, e.g.*, Mark S. Sidolti, *Rule 37(f) – Has This 'Safe Harbor' Provided Any Protection?*, The American Lawyer, Special Sponsor Supplement (December, 2007). But *see* Thomas Y. Allman, *The Role of Good Faith in Managing Information Systems: The Impact of Rule 37(e)*, (June, 2008) that Rule 37(e) has functioned to provide some protection in that "courts reject 'exaggerated sanction claims unless there has been a deliberate manipulation of systems,' and that 'good faith' is emerging as one of the key elements in preservation management.").

[311] Rule 37(f), which became effective on December 1, 2006, was renumbered as Rule 37(e) as part of the 2007 Amendments to the Federal Rules of Civil Procedure. It is referred to as Rule 37(e) throughout this Paper.

Note also that an Advisory Committee Note to the amended Rule specifically cautions that organizations may need to establish credible and defensible litigation hold procedures in order to benefit from this provision.[312]

To date, there are few opinions addressing Rule 37(e). What can be gleaned from those available is that where there is a failure to make any attempt at implementing a litigation hold, there is a presumption that the party did not act in "good faith," thus placing the burden on the party seeking the protection of Rule 37(e) to demonstrate the reasons why it failed to take action to preserve evidence.[313]

11. *Please describe any legal provisions or rules (in place or proposed) that specify the scope of a party's obligation to search for, disclose and produce electronic documents.*

The scope of the obligation to preserve and produce documents in general is addressed above. The 2006 Amended Rules contain specific provisions relating to electronic information, and those are addressed here.

The 2006 Amendments differentiate between "reasonably accessible" and "not reasonably accessible" information in defining the scope of the duty to produce ESI. This provision is commonly referred to as the "two-tiered" rule regarding ESI, meaning that it divides ESI into two "tiers" of ESI, "reasonably accessible" and "not reasonably accessible." The amended Rule 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" (Fed. R. Civ. P. 26(b)(2)(B)). The Advisory Committee Note makes clear that a producing party claiming inaccessibility has certain obligations with respect to the supposedly "not reasonably accessible" information. Among other things, the party must (1) identify the sources of potential information it claims are not reasonably accessible; (2) provide enough detail to allow the opposing party to evaluate the burdens and costs associated with restoring the information; and (3) comply with its obligations to preserve, which may vary depending on the information and the circumstances of the case (*see* 2006 Advisory Committee Note to Fed. R. Civ. P. 26(b)(2)(B)).

Once a party has identified information as not reasonably accessible due to burden or cost, the opposing party may still move to compel discovery of that information.[314] If good cause is shown, the court may order the information produced, with consideration given to sharing or shifting of the costs of restoring the information.[315]

In determining whether or not reasonably accessible information should be produced, the court must consider not only the amount of burden or cost associated with restoring or producing the information, but whether the circumstances of the particular case justify production when balanced against that burden. The Advisory Committee identified the following as among the factors to consider in evaluating this balance:

- the specificity of the discovery request;
- the quantity of information available from other and more easily accessed sources;
- the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;

[312] Fed. R. Civ. P. 37(e) (2006 Advisory Committee Note) ("Good faith may require that a party intervene to modify or suspend certain features of the routine operation of a computer system to prevent the loss of information, if that information is subject to a preservation obligation.").

[313] *See, e.g., Escobar v. City of Houston*, 2007 WL 2900581 (S.D. Tex. Sept. 29, 2007) (finding no showing of bad faith, and refusing to sanction police department for not interrupting its routine system of overwriting electronic information after 90 days).

[314] *See* Fed. R. Civ. P. 26(b)(2)(B) ("On a motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery."

[315] Rule 45 contains the same provision by which a third party may identify information that is not reasonably accessible, and the same allowance that production may still be ordered upon a showing of good cause (Fed. R. Civ. P. 45(d)(1)(D)).

- predictions as to the importance and usefulness of the further information;
- the importance of the issues at stake in the litigation; and
- the parties' resources.[316]

12. *Please describe any legal provisions or rules (in place or proposed) that require a party to verify that a search for electronic documents has been carried out.*

There are no specific obligations with respect to ESI as distinguished from paper discovery.[317] In general, although the party itself need not sign a response to a request for production of documents, that party's counsel must do so. In federal court, such a signature certifies that "to the best of the person's knowledge, information and belief formed after a reasonable inquiry [that] with respect to a disclosure, it is complete and correct as of the time it is made . . ." (Fed. R. Civ. P. 26(g)(1)(A)). Most, if not all, of the states have similar certification provisions.

There are also circumstances related to motions during discovery or summary judgment where a party may be required to submit sworn testimony, either in writing or in person, describing what steps were taken to identify, search for, preserve, and produce documents, and to state that, to the best of the party's knowledge, it has produced all requested information in the party's possession, custody, or control located after a duly diligent search.

13. *Please describe any legal provisions or rules (in place or proposed) that specify how electronic documents should be produced to the other party, including the form of production.*

This is another area that has been addressed by the 2006 Amendments, which were meant to limit squabbles that were occurring where the parties had not been able to reach agreement as to whether documents should be produced in electronic or paper form. Among the new obligatory topics for discussion added to the Rule 26 "Meet and Confer" Conference, discussed above, is the form of production regarding ESI.

Rule 34(b) has also been amended to create default provisions and specific obligations regarding the form in which ESI may be requested and produced.[318] Pursuant to amended Rule 34(b), a requesting party may request a specific form for production. The producing party may choose to produce in that form or may choose instead to object to the requested form. If the producing party objects, it must state the reasons for the objection.

Regardless of whether the requesting party has specified a form, the producing party must, in its written response to the request, state the form or forms in which it intends to produce ESI. Absent an order from the court, or an agreement between the parties, the producing party must produce ESI in either "a form or forms in which it is ordinarily maintained," or in "a form or forms that are reasonably usable" (Fed. R. Civ. P. 34(b)(ii)). Production in a "reasonably usable" form, however, does not give the producing party the right to convert existing ESI from its ordinary form into a form that is less usable for the responding party by, for example, removing or degrading searchability features. The producing party may also be obligated to provide a reasonable amount of technical support or software assistance to allow the requesting party meaningful access (*see* Advisory Committee Note to Fed. R. Civ. P. 34(b)). In addition, absent a showing of good cause, a producing party "need not produce the same electronically stored information in more than one form" (Fed. R. Civ. P. 34(b)(iii)).

[316] 2006 Advisory Committee Note to Rule 26(b)(2)(B).

[317] The 2006 Rules Amendments do include a specific provision allowing parties, upon a showing of specific need, to directly access another party's computers and computer systems (Fed. R. Civ. P. 34(a)). Such may be the case when the court is not convinced that a party has conducted a reasonably diligent search for relevant documents in its possession, custody, or control.

[318] Rule 45 contains the same provisions regarding form or forms of production with respect to subpoenas issued to third parties. The requesting party may seek a specific form(s) of production, and the third party should generally produce in the manner in which the information is ordinarily maintained, or in a reasonably usable form (Fed. R. Civ. P. 45(d)(1)).

14. *What legal standard is applied (e.g., reasonableness, diligence) for the accuracy and completeness of collection, preservation, filtering and production of relevant electronic information?*

The Federal Rules of Civil Procedure impose an affirmative duty on counsel to engage in discovery in a responsible manner, consistent with the spirit and purposes of Rules 26 through 37.[319] That duty is expressed by the "reasonable inquiry" requirement imposed on counsel making, or responding to discovery requests. Fed.R.Civ.P. 26(g)(2) requires that discovery requests, responses or objections must be signed by at least one attorney, and that "[t]he signature of the attorney constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the request, response, or objection is: consistent with the rules and law, not interposed for an improper purpose, and not unreasonable or unduly burdensome or expensive." At least one court has found that a counsel's failure to comply with Fed.R.Civ.P. 26(g)(1) or (2) requires sanctions under Rule 26(g)(3).[320]

At least one court has held that counsel's lack of diligence in searching for sources of information amounted to gross negligence, and imposed sanctions for that conduct.[321]

Additionally, attorneys have ethical obligations that may be triggered by their failure to exercise diligence in collecting, preserving or producing relevant electronically stored information kept by their clients. Rule 3.4 [of the cannons of ethics] states that a lawyer shall not:

> (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;
>
> . . .
>
> (d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party . . . .

15. *Please describe any legal provisions or rules (in place or proposed) that address the treatment of inadvertently disclosed privileged information.*

Significant changes have occurred in the last few years with respect to the law of inadvertent waiver.

First, the 2006 Federal Rules Amendments made changes to the *procedural* law related to privilege and waiver, including a requirement that the parties discuss privilege and waiver issues at the Rule 26(f) "Meet and Confer" Conference,[322] a protocol to follow when privileged information has been inadvertently produced, and a mechanism to bring any unresolved dispute to the court.

Amended Rule 26(f)(4) requires the parties to discuss at the Meet and Confer Conference "any issues relating to claims of privilege or protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order."[323]

---

[319] *See Qualcomm, Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. January 7, 2008).

[320] *See Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354 (D.Md. 2008).

[321] *See Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 WL 1409413, at *5, 8. (S.D.N.Y. May 23, 2006).

[322] Amended Rule 26(f)(4) states that parties should discuss "any issues relating to claims of privilege or protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order."

[323] There are two general types of agreements parties might make regarding privilege. The first is known as a "quick peek" agreement, pursuant to which a party may produce a batch or sample of a particular type of information requested by the other party, with the agreement that any privileged information so produced is not subject to waiver. After a brief review, the requesting party returns the information and designates the specific information or documents it wants actually produced. The second type of agreement allows a party to retrieve inadvertently produced privileged documents and is known as a "clawback" agreement. The "clawback" agreement is similar to the procedure outlined in Rule 26(b)(5), and it permits a party that mistakenly produces privileged information to identify and retrieve the materials upon timely notice to the receiving party, without waiver of the inadvertently produced information. *See* 2006 Advisory Committee Note to Fed. R. Civ. P. 26(f)(4). Both the "quick peek" and the "clawback" agreement are inherently risky and infrequently used. Simply put, there is no risk-free way to enter into either form of agreement that does not potentially jeopardize the client's or counsel's interests in present or future litigation.

Amended Rule 26(b) outlines a protocol by which a party may identify an inadvertently produced privileged document. Pursuant to that protocol, if privileged information is produced inadvertently, "the party making the claim may notify any party that received the information of the claim and the basis for it." After being so notified, the receiving party "must promptly return, sequester or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved" (Fed. R. Civ. P. 26(b)(5)).

Second, on September 19, 2008, Federal Rule of Evidence 502 was enacted, which places limitations on the waiver of the attorney-client privilege and work product protections. Rule 502 was passed partially in "response to the costs involved in extensive document review necessitated by electronic discovery."[324] Its supporters hoped Rule 502 would provide more predictable, uniform standards under which parties can determine the consequences of disclosing a communication or information covered by the attorney-client privilege or work product protection.[325]

Rule 502 has several provisions that effect waiver of privilege and the inadvertent production of privileged materials in federal court proceedings and before federal agencies. Section (a) states that privilege will not be waived as to undisclosed privileged materials (*i.e.,* subject matter waiver) because of the inadvertent production of other privileged materials.[326] Section(b) prohibits the waiver of privilege of disclosed materials where the production was inadvertent and the disclosing party took both reasonable steps to prevent production and reasonably prompt steps to rectify the production (*see* Rule 502(b)). Additionally, Rule 502 holds that federal court orders on the disclosure and waiver (or non-waiver) of privileged documents are binding on other federal *and state* courts, while agreements between parties on the same issues are binding only on themselves (*see* Rule 502 (d) and (e)).

Rule 502 does not define "inadvertent disclosure," but the Advisory Note to Rule 502 summarizes the multi-factor test used by the majority of courts:

> The stated factors (none of which are dispositive) are the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issues of fairness. The rule does not explicitly codify the test, because it is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those listed factors.[327]

16. *Please describe how the costs of electronic information disclosure are dealt with in this jurisdiction.*

Obligations relating to the costs of discovery are addressed above. Particulars with respect to the cost of electronic discovery are addressed here. In the US, this area of the law is known as "cost shifting," in reference to the default position that the producing party typically bears the costs of discovery, and that costs will not be shifted in the typical situation.

Although the Rules do not directly address cost shifting, the topic has been covered in a number of earlier court rulings. The leading case in this area is, again, *Zubulake v. UBS Warburg LLC*, in which the court built upon and then substantially revised the law.

Although other courts had fashioned a test to determine when cost-shifting should occur, the *Zubulake* court's first innovation was to condition when the test should be applied, noting that cost shifting is not appropriate in every case. The court reasoned the concept that "an undue burden or expense may arise simply because

---

[324] *Containment Tech. Group v. American Soc. of Health Sys. Pharmacists*, 2008 WL 4545310, *4 (S.D. Ind. Oct. 10, 2008) (citing Fed. R. Evid. 502 Advisory Note).
[325] *See* Explanatory Note on Evidence Rule 502 Prepared by the Judicial Conference Advisory Committee on Evidence Rules.
[326] *See* Rule 502(a)(i) (requiring intentional waiver to cover undisclosed materials).
[327] *Id. See also Laethem Equipment Co. v. Deere and Co.*, 2008 WL 4997932 (E.D. Mich. Nov. 21, 2008); *Rhoads Industries, Inc. v. Building Materials Corp.*, 254 F.R.D. 216, 219 (E.D. Pa. 2008).

electronic discovery is involved . . . makes no sense."[328] "Electronic evidence is frequently cheaper and easier to produce because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying."[329] Referencing the distinction between "accessible" and "inaccessible" data described earlier in this article, the court held that it was appropriate to consider cost-shifting with respect to "inaccessible" data only.[330] This was so because inaccessible data, meaning backup tapes and "erased, fragmented, or damaged data," was not stored in a "readily useable format" and had to be restored, de-fragmented, or reconstructed before it could be usable.[331] Hence, it was appropriate to consider cost-shifting with respect to such efforts only, but not with respect to accessible data, which is more easily obtained.

Next, although the *Zubulake* court recognized the factors laid down in an earlier case as "the gold standard," the court chose not to follow them because they undercut the presumption, set forth in the Federal Rules and reiterated by the Supreme Court, "that the responding party must bear the expense of complying with discovery requests . . . ."[332] The *Zubulake* court reconfigured the *Rowe* factors, adding some factors that were not included even though they were specifically identified in Rule 26(b)(2), combining and deleting others because they were unimportant or redundant, and weighting certain factors that the court felt should predominate. The end result was the following seven factor test, weighted in diminishing order of importance.

1. the extent to which the request is specifically tailored to discover relevant data,
2. the availability of that data from other sources,
3. the total cost of production relative to the amount in controversy,
4. the total cost of production relative to resources available to each party,
5. the relative ability and incentive for each party to control its own costs,
6. the importance of the issues at stake in the litigation, and
7. the relative benefits to the parties in obtaining that data.[333]

The court also noted that the first two factors, comprising a "marginal utility test," were the most important.

The final *Zubulake* innovation was to insist that the test not be applied in a factual vacuum. The court set forth a three-step factual analysis that needed to take place before a court could resolve disputes concerning the scope and cost of electronic discovery:

> *First,* it is necessary to thoroughly understand the responding party's computer system, both with respect to active and stored data. For data that is kept in an accessible format, the usual rules of discovery apply: the responding party should pay the costs of producing responsive data. A court should consider cost-shifting *only* when electronic data is relatively inaccessible, such as in backup tapes.
>
> *Second,* because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases.[334]

---

[328] *Zubulake I*, at 318.
[329] *Id.*
[330] *Id.* at 318-20.
[331] *Id.* at 320.
[332] *See Zubulake I*, at 316 (quoting *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978)).
[333] *See id.* at 322-23.
[334] This "accessible" and "inaccessible" distinction was followed by the New Rules with respect to the two-tiered approach set forth in Rule 24(b)(2), as discussed above.

> *Third,* and finally, in conducting the cost-shifting analysis, the [court should consider the factors set forth above].[335]

The cost-shifting standard set forth by the *Zubulake* court has been followed by the majority of courts that have subsequently addressed the issue of cost-shifting.[336]

17. *Are information management policies and procedures, including records retention schedules and legal hold notices used to ensure the preservation of electronic information for business and legal purposes?*

Many public entities and private organizations are subject to regulatory requirements governing the retention of information.[337] Retention regulations are imposed on some organizations by the SEC and NASD; other organizations must retain records for purpose of tax, employment and environmental laws.[338]

A 2007 survey indicated that 89% of U.S. companies had litigation hold policies in place.[339] According to that survey, almost all companies of $1 billion or more in revenues (98%) had such policies.[340] Yet another survey, however, indicated that 65% of companies had no records management policy.[341]

Where used, legal hold notices typically 1) identify the persons who are likely to have relevant information; 2) are in written form and designed to effectively communicate the requirement to preserve information; 3) clearly define what information is to be preserved and how preservation is to be undertaken; and 4) are periodically reviewed, and reissued.[342] Because litigation hold policies and the process of implementing legal holds are often in written form, the process may be subject to scrutiny by opposing parties and courts.[343]

18. *Is there widespread use of electronic information management technologies within your jurisdiction to assist with the preservation, classification, and management of electronic information for legal reasons?*

The explosion of electronically stored information has fostered the creation and use of a wide array of tools to assist with electronic discovery. New and enhanced technologies are used throughout the United States to assist with preservation and production issues associated with electronic information. With respect to data production, these tools assist with data harvesting and filtering, data conversion and processing for review (creating images or html renderings for native review), email processing and redaction of privileged material.[344] Technological solutions are also being developed and used to archive and restore electronic information, to search and retrieve responsive information, and eliminate duplicate email files.[345]

Emerging technologies are being developed to address accessibility issues related to electronically stored information on backup tapes. These innovations make it possible to perform full content and metadata indexing at the speed of tape, thereby avoiding full backup tape restoration. The index can then be searched, limiting restoration to only the data actually needed.[346]

---

[335] *Id.*
[336] *See* Shira A. Scheindlin & Jonathan M. Redgrave, "Discovery of Electronic Information," 2 *Business and Commercial Litigation in Federal Courts 2d*, §§ 22.64–22.65 (Robert L. Haig ed., 2005 & Supp. 2007).
[337] *See The Sedona Conference Commenatary on Email Management: Guidelines for the Selection of Policy*, *Public Comment Draft*, August 9, 2006, at p. 12.
[338] *Id*.
[339] *See* Fourth Annual Litigation Trends Survey, Fulbright & Jaworski L.L.P., 2007 at 25.
[340] *Id*.
[341] *See* "Many organizations lack records retention policies, survey shows" October 12, 2007 Compliance News, www.itcinstitute.com.
[342] *See The Sedona Conference Commentary on Legal Holds* at p. 4. *See also Zubulake IV*, at 212; *Samsung Electronics Co., Ltd., v. Rambus Inc.*, 439 F. Supp. 2d 524, 565 (E.D. Va. 2006) (imposing duty on organization to "inform its officers and employees of the actual or anticipated litigation and identify for them the kinds of documents that are thought to be relevant to it.").
[343] *Id*.
[344] For a discussion of considerations when selecting vendors that offer these tools, *see The Sedona Conference, Best Practices for the Selection of Electronic Discovery Vendors*, June 2007.
[345] *See generally, The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, Sedona Conference Journal, Vol 8, August 2007.
[346] Gerald Britton and Richard Davis, *New Technology Alters the Terrain on Accessibility of Backup Tape Data*, Law Technology Today (June 2007).

Lawyers in the U.S. are using increasingly sophisticated search and retrieval tools to address ever-increasing volumes of electronically stored information. While the use of these tools is relatively recent,[347] they are becoming widespread in cases with voluminous ESI production. The most commonly used search tool (Boolean) is based on the use of "keywords" and "operators" (*e.g.,* "AND," "OR" and "AND NOT" or "BUT NOT").[348] Metadata is also used to assist with keyword searching.[349] Other searching tools – Bayesian, fuzzy searching, clustering and concept-based searching – are also used depending on the type of data produced, the sophistication of the parties and other factors.[350]

19. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

No one unilateral legal framework for privacy exists in the United States. Historically privacy rules in the U.S. have been sector-based along with federal and state case law and common law. The sector-based approach grew out of government interest to protect personal consumer information, particularly when used by third parties for commercial purposes. Sector-based privacy rules exist in such areas as credit, finance, health, online children activities, online marketing and telemarketing, and they continue to grow on both a state and federal level.

U.S. privacy rules have also developed through constitutional, contract, and tort law, and corresponding case law. Though no express right to privacy has been found in the U.S Constitution, the U.S. Supreme Court has found limited implied constitutional rights to privacy in many areas. Some ten states have expressly added a right to privacy to their state constitutions – California being one of them.[351]

While applied on only a sectoral basis, the fundamental principles of U.S. privacy law reflect the 1980 Organization for Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and the more recent Privacy Framework established by the Asia-Pacific Economic Cooperation (APEC) member countries. These principles include rights concerning "notice" and "choice," which require that individuals be informed as to how personally identifiable information about them will be used and enable those individuals to opt-in or opt-out of specific uses of their personal information. They also include a right to the implementation of adequate security safeguards for the protection of non-public personal information. In this regard, there has been a recent growth in state laws requiring notification to affected individuals of breaches of personal information. At least 44 states now have such data breach laws, which are intended to protect against identity theft and fraud. State data breach laws function implicitly if not explicitly as state-based privacy rules.

Most U.S. privacy laws, both federal and state and regardless of sector, permit uses and disclosures of personal information for law enforcement, public health and safety purposes. Additionally, a right to access or obtain protected data may be available through judicial process, including via subpoenas and court orders. Generally, a court must weigh the potential relevance of the requested information against the privacy interests at stake. In doing so, the court may take one or several of the following actions: issue a protective order; conduct proceedings *in camera*; require parties to execute a non-disclosure agreement; order data be de-identified, anonymized or destroyed post-matter; limit and narrow the scope of disclosure; order full disclosure; or entirely squash the subpoena or motion for disclosure.

There are numerous federal statutes that establish obligations to maintain the privacy of certain types of personal information. A sampling of some of the more significant of these laws is highlighted below.

---

[347] *The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, The Sedona Conference Journal, Vol. 8, (2007) at 197.
[348] *Id*.
[349] *Id*. at 201.
[350] *Id*. at 217.
[351] *See* National Conference of State Legislatures, "Privacy Protections in State Constitutions," *available at* http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited Dec. 1, 2008).

Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act of 1999 (GLBA) establishes that a financial institution has "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information" (15 U.S.C. § 6801(a)). With limited exceptions, the GLBA prohibits a financial institution from disclosing a customer's non-public personal information unless the customer has been given notice and the customer fails to opt out of an information-sharing arrangement (15 U.S.C. § 6802). Section 6802(e)(8) of the act permits disclosure in order to respond to judicial process. Courts have held this clause to mean that "[a] financial institution [may] disclose the non-public personal financial information of its customers to comply with a discovery request."[352]

The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of individually identifiable health information used and maintained by healthcare providers, health plans, and certain other entities. The Department of Health and Human Services has implemented detailed regulations that restrict uses and disclosures of identifiable health information by entities covered under the statute. Under the statute, identifiable health information may be disclosed in response to a discovery request so long as the request is accompanied by a court order, the individual who is the subject of the data has received notice of the request and has had an opportunity to object, or the parties agree to a protective order stipulating that the information will only be used for the purposes of the litigation and that the information will be returned or destroyed at the conclusion of the litigation.[353]

The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) is designed to protect the privacy of credit report information and guarantee that information supplied by consumer reporting agencies is as accurate as possible. The FCRA, whose implementation is overseen by the Federal Trade Commission, prohibits consumer reporting agencies from sharing a consumer's report with a third party without authorization from the consumer, unless the disclosure is for one of several enumerated permissible purposes (15 U.S.C. § 1681b). Among these permissible disclosures, a credit reporting agency may share a consumer's report without authorization if it is acting "in response to the order of a court having jurisdiction to issue such an order or a subpoena issued in connection with proceedings before a Federal grand jury" (15 U.S.C. § 1681b (a)(1)).

The Drivers Privacy Protection Act

The Drivers Privacy Protection Act (DPPA) limits release and use by any state of personal information obtained through the state's motor vehicle records of individuals. The Act was amended in 2000 to require an individual's affirmative consent to be obtained before the state may release his or her personal information to a third party for marketing purposes. The Act allows disclosure of a driver's motor vehicle records for litigation and court proceedings. Many states have enacted their own laws regulating motor vehicle records. Some of these state laws do not allow for release of the records for litigation and court proceedings.

The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) is aimed at maintaining the confidentiality of personal information collected from children under the age of 13. COPPA requires operators of websites and online

[352] *Marks v. Global Mortgage Group, Inc*., 218 F.R.D. 492, 496 (S.D.W. Va. 2003); *see also Her v. Regions Fin. Corp.*, 2007 WL 2806558, at *2 (W.D. Ark. Sep. 25, 2007).
[353] *See* 45 C.F.R. § 164.512(e)(1); *see also U.S. ex rel. Camillo v. Ancilla Sys., Inc*., 233 F.R.D. 520, 522 (S.D. Ill. 2005); *Crenshaw v. MONY Life Ins. Co*., 318 F. Supp. 2d 1015, 1029 (S.D. Cal. 2004).
[354] *See Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 450 (C.D. Cal. 2007); *see also Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 877 (9th Cir. 2002).

services to establish and maintain reasonable procedures to "protect the confidentiality, security, and integrity of personal information collected from children" (15 U.S.C. § 6502(b)(1)(D)). Before collecting, using or disclosing a child's personal information, a web site operator must obtain verifiable consent from the child's parent. The statute allows for the disclosure of a child's personal information to that child's parent. Section 6502(b)(2)(E)(iii) of the Act permits operators to use or disseminate personal information without parental consent when responding to judicial process. The Federal Trade Commission is responsible for implementation of COPPA.

The Stored Communications Act

The Stored Communications Act (SCA) prohibits electronic communication service providers from knowingly divulging the contents of any communication stored on that service to a third party unless in compliance with a court order issued by a court of competent jurisdiction (18 U.S.C. §§ 2702(a)(1), 2703(d)). Likewise, the Wiretap Act prohibits the intentional disclosure of information that was obtained via the interception of "a wire, oral, or electronic communication" (18 U.S.C. § 2511(1)(c)). Both the SCA and the Wiretap Act are part of the Electronic Communications Privacy Act (ECPA), which governs oral, wire, and electronic communications. The SCA addresses authorized access to stored information, and the Wiretap Act addresses unauthorized access to intercepted communications. As such, "an electronic communication may not simultaneously be actionable under both the Wiretap Act and the SCA."[354] The SCA permits a provider to disclose the contents of any wire or electronic communication to a governmental entity without notice to the subscriber if in response to a court order. The order may issue "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation" (18 U.S.C. §§ 2703(b)-(d)). The Wiretap Act allows for intercepted electronic communications to be made available for discovery, even if the communications may later be found inadmissible.[355]

Workplace privacy is also regulated at the federal and state level. The Department of Labor, the Federal Trade Commission, and the Equal Employment Opportunity Commission are the primary federal agencies that govern workplace privacy. Monitoring, surveillance and reporting are generally permissible business practices in the U.S. workplace. These activities must be for legitimate business purposes and executed in conjunction with reasonable procedures. As technology increases the ability to monitor employee activity in the workplace, however, there is a growing demand for employers to provide notice of their workplace privacy policies. For example, Connecticut and Delaware have both enacted laws requiring employers to provide notice of their electronic monitoring practices.[356] In the absence of such a state statute, an employer's stated workplace privacy policy, consistency of practices, enforcement of policy, training and consent are important factors that substantiate an employer's right to monitor.[357]

In addition to federal and state statutes, common law privacy principles may also affect a business's obligation to maintain the security and privacy of employee records. For example, one court has held that employees have an "expectation of privacy" in information maintained on their office computers.[358] In *Leventhal v. Knapek*, while the court recognized an expectation of privacy in materials stored on an office computer that was for the employee's exclusive use, it ultimately held that an employer's search of the computer for "evidence of suspected work-related employee misfeasance will be constitutionally reasonable if [the search] is justified at its inception and of appropriate scope."[359] When considering the scope of the SCA, an expectation of privacy

[355] *McQuade v. Michael Gassner Mech. & Elec. Contractors, Inc*., 587 F. Supp. 1183, 1190 (D.C. Conn. 1984) (stating, "[t]he possible inadmissibility of the tape recordings at trial is not an adequate reason to foreclose discovery of them. . . . Since disclosure of the tape recordings is not proscribed until a violation of § 2511 is shown, it follows that they are discoverable for the time being, subject perhaps to an appropriate order protecting the arguable privacy interests of relevant parties.").

[356] *See* 19 Del C. § 705; Conn. Gen. Stat. § 31-48d.

[357] *See Biby v. Board of Regents*, 419 F 3rd 845 (8th Cir. 2005); *TBG INS Serv.Corp.v. Superior Court*, 96 Cal. App. 4th 433; *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007).

[358] *See Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001).

[359] *Id*. at 75.

[360] *Available at* http://www.hhs.gov/hipaafaq/permitted/law/505.html.

would only apply to information on the hard drive of an exclusive use computer. Any information stored on a shared computer, shared drive, or distributed over a network would not implicate the same privacy expectations. Cases such as *Leventhal* that have found an expectation of privacy in the workplace are fact sensitive and limited, and they should be viewed more as the exception than the rule.

Some sector-based laws, particularly in the banking and securities industry, *actually require* employers to monitor and/or report the activities of their employees and customers. Such laws include the Bank Secrecy Act of 1970, The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), the International Money Laundering Act of 2001, and the U.S. Communications Assistance to Law Enforcement Act of 1994 (CALEA). The Securities and Exchange Commission also has promulgated regulations that require surveillance of certain customer and employee activities in furtherance of protecting investors and the public.

Finally, public sector privacy rules such as the Privacy Act of 1974 regulate Federal government access to and use of U.S. citizen and legal residents' information. The purpose of the statue was to establish appropriate fair practices for the use of personal data stored by the government. In particular, the Act was also intended to limit the use of social security numbers (SSNs). The Freedom of Information Act (FOIA) allows individuals to access federal government records but excludes access to certain protected information, including information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Nevertheless, even if information is deemed protected, there are processes available through the courts to provide for disclosure when and if necessary.

Electronic Data Protection and Privacy

20. Please describe your country's approach to electronic data protection and privacy. Please include in your response:

a. The purposes, origins, and guiding principles for any data protection and privacy legislation, regulation or contract in your jurisdiction. (Please attach the most recent version of country specific data protection or privacy legislation.)

There is no one approach to electronic data protection and privacy in the United States. As described above, privacy law in the U.S. is neither a single piece of legislation nor an overarching federal legal framework. Components of privacy law are found implicit in the federal constitution, explicit in some state constitutions, in case law, common law, tort, and contract, federal and state legislation and regulation – basically across the full panoply of legal processes and venues available in the United States.

Historically this sector-based approach to privacy grew out of an interest in managing the fair use of consumer information and specifying permissible purposes that would allow for the use of non-public personal consumer information. The Federal Trade Commission oversees consumer protection and the use of personal information in most business sectors – except where other regulatory agencies have sector-based authority. The FTC's authority in the area of privacy stems from Section 5 of the U.S. Federal Trade Commission Act, which prohibits unfair and deceptive acts or practices in commerce. The FTC uses this authority to ensure that the statements that a business makes concerning its data privacy and security practices are truthful and that appropriate security safeguards have been implemented to protect sensitive personal information.

The Code of Fair Information Practices (also known as the Code of Fair Information Principles) is a foundation to many U.S. privacy laws. The Code was developed in 1970 by an Advisory Committee on Automated Systems of the U.S. Department of Health, Education and Welfare. The Code consists of the following principles: openness, individual participation, collection limitation,

data quality, finality, security and accountability. Notice and choice are fundamental to sector-based privacy requirements in the U.S. Pursuant to these principles, organizations must post privacy policies, comply with these policies, and provide effective processes to allow consumers to opt-in or opt-out of additional use of their non-public personal information.

Privacy obligations are also managed through contract law. Many sector-based privacy regulations (*e.g.,* regulations under GLB and HIPAA) require regulated entities to contractually obligate third-party vendors to implement privacy and security safeguards. In the U.S. there is a growing practice even among non-regulated entities to impose privacy and security requirements on service providers. Non-disclosure and /or confidentiality agreements are also used to ensure confidentiality and privacy protections.

The spread of state data breach notification laws and accompanying increase in reporting of data loss incidents have given rise to causes of action in negligence for data breach. Data breach claims in negligence have largely failed to date due to the difficulty in establishing damages and/or standing.

b. The legal definition of "personal data" and "processing" of data within your jurisdiction.

There is no single definition of "personal data" in the U.S.

State breach notification laws often define personal information as an individual's first name or first initial and last name in combination with one or more of the following data elements: social security number; driver's license or state identification card number; or financial account number in combination with any required pin number or password. The breach notification laws usually apply only to personal information in electronic form and exclude encrypted information. However, several states have broader definitions of what personal data they protect under their data breach notification laws, and the requirements of each state must be researched if an organization experiences a breach.

Sector-based rules have their own definitions of what data is subject to protection. Examples include the following:

- GLBA refers to "non-public personal information" (NPI). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."

- FCRA refers to "consumer reports." A consumer report is "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit-worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living."

- HIPAA refers to "protected health information" (PHI). PHI is defined as individually identifiable information that relates to the individual's past, present or future physical or mental health; the provision of health care to the individual; or the past, present or future payment for health care. Information is considered individually identifiable if it could be used, either alone or in combination with other information, to identify an individual.

Privacy laws in the U.S. do not use the term "processing" of personal data; however, similar concepts exist. For example, the HIPAA Privacy Rules specify for what purposes the "use" or "disclosure" of protected health information is permitted. "Use" is defined as "the sharing,

employment, application, utilization, examination, or analysis" of PHI. "Disclosure" is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." However, because there is no omnibus U.S. privacy law, terminologies and definitions differ by sector.

c. *What, if any, privacy rules are there in your jurisdiction which impact on the disclosure/production of documents, including electronic documents, in legal proceedings or regulatory enquiries (commenced in your jurisdiction or in other jurisdictions which can be enforced in your jurisdiction)?*

Again, because there is no omnibus U.S. privacy law, matters that require disclosure of protected personal information need to be reviewed and assessed on a case-by-case basis to determine what exceptions apply or approval processes need to be followed to enable appropriate legal disclosure of such information. Generally, most U.S. privacy laws include exceptions that permit disclosures required by law, disclosures necessary for law enforcement purposes, and disclosures for public health and safety.

d. *Whether data protection and privacy legislation, regulation or contracts in your jurisdiction apply to both civil and criminal proceedings.*

Most U.S. privacy laws include exceptions that permit disclosures of personal data for purposes of both civil and criminal proceedings, provided certain criteria are met or procedures are followed. These criteria and/or procedures can be quite detailed. For example, Frequently Asked Questions concerning the HIPAA Privacy Rule address the following:

> When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?[360]
>
> . . .
>
> **To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.** The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information (45 CFR 164.512(f)(1)(ii)(A)-(B)).
>
> **To respond to an administrative request**, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).
>
> May a covered entity that is not a party to a legal proceeding disclose protected health information in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order?[361]
>
> Yes, if certain conditions are met. A covered entity that is not a party to litigation,

[361] *Available at* http://www.hhs.gov/hipaafaq/permitted/judicial/711.html.

such as where the covered entity is neither a plaintiff nor a defendant, may disclose protected health information in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order, provided that the covered entity:

- Receives a written statement and accompanying documentation from the party seeking the information that reasonable efforts have been made either (1) to ensure that the individual(s) who are the subject of the information have been notified of the request, or (2) to secure a qualified protective order for the information; or

- Itself makes reasonable efforts either (1) to provide notice to the individual(s) that meets the same requirements as set forth below for sufficient notice by the party making the request, or (2) to seek a qualified protective order as defined below. *See* 45 CFR 164.512(e).

The covered entity must make reasonable efforts to limit the protected health information used or disclosed to the minimum necessary to respond to the request. *See* 45 CFR 164.502(b) and 164.514(d).

The requirement to provide sufficient notice to the individual(s) is met when a party provides a written statement and accompanying documentation that demonstrates:

- A good faith attempt was made to notify the individual (or if the individual's location is unknown, to mail a notice to the individual's last known address);

- The notice included sufficient detail to permit the individual to raise an objection with the court or administrative tribunal; and

- The time for the individual to raise objections under the rules of the court or tribunal has lapsed and no objections were filed or all objections filed by the individual have been resolved by the court and the disclosures being sought are consistent with the resolution.

A qualified protective order is an order of a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and requires the return to the covered entity or destruction of the protected health information (including any copies) at the end of the litigation or proceeding. The party requesting the information must provide a written statement and accompanying documentation that demonstrates:

- The parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or

- The party seeking the protected health information has requested a qualified protective order from the court or administrative tribunal.

e. Whether natural and legal persons have rights under data protection and privacy legislation, regulation or contracts in your jurisdiction.

Generally, U.S. sector-based privacy rules apply only to natural persons. Contract, tort and common law may provide legal remedies for legal entities in addition to natural persons.

f. Any exemptions from the applicability of data protection and privacy legislation, regulation or contract in your jurisdiction.

Four key federal laws compel disclosure of personal information over privacy rights: the Bank Secrecy Act of 1970, the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), the International Money Laundering Act of 2001, and the U.S. Communications Assistance to Law Enforcement Act of 1994 (CALEA). These laws require reporting, surveillance and monitoring of business and financial information with the objective of protecting U.S. security and preventing activities that support money laundering and terrorism. These laws require banking organizations to 'know their customer', monitor customer account activity and report suspicious transactions.

The Bank Secrecy Act requires financial institutions to monitor currency transactions and report suspicious activity. The USA Patriot Act authorizes financial institutions to monitor, survey and share information with the government for purposes of protecting against money laundering and terrorist activity. The International Money Laundering Act increases surveillance duties and other investigative responsibilities in relation to protecting national secrecy and preventing terrorism. CALEA requires the cooperation of telecommunication carriers with government efforts to intercept and monitor communications for law enforcement, security and safety purposes – at present VOIP is not considered to be covered by this act.

Other U.S. agencies that are charged with protecting certain public interests may compel disclosure of protected information in certain circumstances. The Food and Drug Administration (FDA), the U.S. Department of Labor's Occupational Health and Safety Administration (OSHA) and the U.S. Department of Health and Human Services are three examples of agencies that are empowered to compel disclosure of protected information.

g. Any specific data types, subject areas or situations for which electronic discovery is restricted.

As a general matter, electronic discovery laws and rules do not restrict the production of relevant information by data type or subject area, with the significant exception of certain communications with attorneys or attorney work product. There are situations where the information is considered to be difficult to obtain because of cost, such as back-up tapes, in which case electronic discovery law and rules provide that a Court should consider the importance of the information to the case in determining if the information need be produced and who should bear the cost of such production. Certain types of data are protected by data protection and privacy legislation, such as those set forth in answer to question 19 above. A court will consider those provisions which apply. In many situations, a party to a matter will be considered to have waived its right to assert such provisions on its own behalf.

h. Any employee, employer, union or other contractual considerations related to electronic data and discovery.

As a general matter, there are no contractual considerations relating to electronic discovery regarding employee, employer or union data. Where such information is relevant to the issues in a litigation, it is considered subject to production. It is possible that in a given matter, a contractual provision may apply to certain data that requires notice to a non-party whose data is sought of the request for its production, so as to provide them an opportunity to object to its production. As a general matter, such objection will be evaluated based upon the privacy interest asserted against the importance of the information to that litigation.

i. A description of the role of notice to the regulating agency, data subject, or others, under any applicable law in your country.

There is no general requirement that an organization notify its regulating agency of its data processing activities. Notification to government agencies may be required if an organization experiences a breach of personal data, pursuant to state breach notification requirements or sector-specific federal law.

Obligations to notify data subjects of an entity's data processing activities vary by sector.

j. A description of the established procedures for obtaining information for processing or transfer of personal data for the purposes of litigation, regulatory or internal investigations.

There are no uniform procedures for obtaining information for processing or transfer of personal data for purposes of litigation, regulatory or internal investigations. For an example of procedures to be followed under HIPAA, see question (d) above.

k. Whether your jurisdiction acknowledges the validity of employee consent for the processing and transfer of personal data. If so, what are the requirements for such consent? (Please attach country approved exemplar if available.)

Generally speaking, consent is considered a valid basis for the processing and transfer of personal data in the United States, including consent given by an employee.

Cross-border Discovery

21. Please describe the law pursuant to which foreign litigants may attempt to obtain discovery from subjects in your country. Please include in your response:

a. Whether the Hague Convention is the exclusive process for conducting cross-border discovery in your jurisdiction.

No, the Hague Convention is not the exclusive process for conducting cross-border discovery in the U.S. Section 1782 of Title 28 of the United States Code is a federal statute that allows a party to a legal proceeding *outside* the United States to apply to an American Court to obtain evidence for use in the non-US proceeding. The full name of Section 1782 is the "Assistance to foreign and international tribunals and to litigants before such tribunals."

The text of Section 1782(a) reads as follows:

> The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations

> conducted before formal accusation. The order may be made pursuant to a letter rogatory issued, or request made, by a foreign or international tribunal or upon the application of any interested person . . . . The order may prescribe the practice and procedure, which may be in whole or part the practice and procedure of the foreign country or the international tribunal, for taking the testimony or statement or producing the document or other thing. To the extent that the order does not prescribe otherwise, the testimony or statement shall be taken, and the document or other thing produced, in accordance with the Federal Rules of Civil Procedure.

The type of evidence that may be obtained under Section 1782 includes both documentary evidence and testimonial evidence.

The laws of various States may also allow for discovery without resort to the Hague Convention.

b. If your country has a blocking statute, has it ever been enforced? If so, please provide details of the enforcement.

No, the U.S. does not have a blocking statue. However, there are restrictions on the transfer of certain information implicating U.S. defense interests.

c. What factors are considered in permitting cross-border discovery (e.g., significant contracts, whether the requesting jurisdiction is subject to EU Directive)?

In essence, an applicant under Section 1782 noted above merely needs to show three things: (a) it is an "interested person" in a foreign proceeding, (b) the proceeding is before a foreign "tribunal," and (c) the person from whom evidence is sought is in the district of the court before which the application has been filed. State laws vary.

Appendix A: The Sedona Conference® Working Group Series & WGS℠ Membership Program

"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY"

The Sedona Conference® Working Group Series ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGS℠ begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production (March 2003 version)—was immediate and substantial. The Principles was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's Digital Discovery and E-Evidence, "The Principles...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) Markman hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. See the "Working Group Series" area of our website www.thesedonaconference.com for further details on our Working Group Series and the Membership Program.