

# **Guidelines for the Discovery of Electronic Documents in Ontario**

*A Supplemental Report of*

**The Task Force on the Discovery Process in Ontario**

**October, 2005**

*Compliments of*



## GUIDELINES FOR THE DISCOVERY OF ELECTRONIC DOCUMENTS IN ONTARIO

### **A. Introduction: Purpose of E-Discovery Guidelines**

In its Report, the Task Force on the Discovery Process in Ontario recommended the development of a “best practices” manual to address the discovery of electronic documents. These Guidelines respond to that recommendation.<sup>1</sup>

The preservation, retrieval, exchange and production of documents from electronic sources in electronic form are together referred to as “e-discovery.” In these Guidelines, that term also includes the use of automated tools to produce documents in electronic form, whether they originate in hard copy or electronic sources. While documents from hard copy sources can be produced in electronic form, and paper copies of electronic documents can be printed out for production in litigation, these activities would not, in themselves, constitute “e-discovery” as the term is used, generally or in these Guidelines.

The development of best practices for e-discovery is not unique to Ontario. A number of other organizations and jurisdictions have implemented or published similar guidelines that have been instructional in the development of these Guidelines. These are referred to as appropriate in the commentary.

The premise of these Guidelines is that existing Rules already provide a legal foundation for the requirement that parties address issues relating to e-discovery, because the definition of “document” in applicable civil Rules already includes “data and information in electronic form.”<sup>2</sup> However, those Rules and the case law to date provide little clear guidance to parties and their counsel on *how* to fulfill that requirement. The suggestions in these Guidelines have been developed to address this issue with respect to production of documents in civil litigation.

E-discovery is already widely used as an integral part of the discovery process in complex cases and, increasingly, in many types of litigation that are less complex. In part, this is because of the inclusive definition of “document” referred to above. In addition, however, as the available technology matures, lawyers have begun to recognize its capacity, in some cases, to manage document production more efficiently, and to support the discovery process more effectively, than traditional paper-based methods permit.

However, many lawyers have yet to fully recognize the impact of this technology on the discovery process. The overall orientation of the profession remains towards printed documents. This, combined with the absence of clear guidelines on the scope and manner of e-discovery, means that many lawyers remain unfamiliar with their clients’ obligations to preserve and produce electronic documents, and with the technology available to retrieve, search and produce them in a cost-effective manner.

Accordingly, Section C below sets out a number of principles that are intended to guide lawyers, clients and the judiciary in the e-discovery process. It is hoped that these Guidelines will provide an appropriate framework to address *how* to conduct e-discovery, based on norms that the bench and bar can adopt and develop over time as a matter of practice. They are not intended to be enforceable directly, as are the *Rules*

---

<sup>1</sup> The Discovery Task Force wishes to thank the members of the e-Discovery Sub-Committee for their excellent work: Sara Blake, Martin Felsky, Michael Fraleigh, Derek Freeman, Karen Groulx, Christopher Leafloor, Daniel Pinnington, Glenn A. Smith, Phil Tunley and Mohan Sharma.

<sup>2</sup> Rules of Civil Procedure, Rule 1.03

*of Civil Procedure*, although they may support the enforcement of agreements between parties or provide the basis for court orders. Mandating how e-discovery is conducted through the enactment of detailed rules, at this stage, could be counterproductive, and risk imposing a “one-size fits all” approach that may not be appropriate in different types of litigation or responsive to new technologies as they emerge. It could also add unnecessary complexity to the Rules, and lead to more disputes and related motions.

Rather, the objective of these Guidelines is to educate the legal profession, including the judiciary and the practicing bar, on issues relating to e-discovery and how those issues can be addressed in practice. They are intended to provide practical suggestions for the profession, both on how to fulfill parties’ existing obligations respecting the preservation and production of relevant documents from electronic sources, and how to improve the cost effectiveness of the discovery process. They suggest how to reach early agreements in the e-discovery process, in order to minimize the potential for undue cost and delay.

These Guidelines also include some suggestions to take advantage of electronic tools, in order to minimize unnecessary cost and delay. Despite the apparent complexity of some e-discovery issues, technology increasingly offers improved methods of retrieving, reviewing and producing documents electronically. In many circumstances, this can offer significant savings of cost and time compared to paper-based methods.

In order to serve as an educational guide for the profession, it may be necessary for some readers to review the basic concepts and terminology relating to e-discovery. For those readers, Section B following provides this review in a practical context. It outlines the stages in the process of discovery of electronic documents, and some key terminology and concepts that lawyers and judges need to master at each stage.<sup>3</sup> Those readers who are already familiar with this terminology and the e-discovery process may prefer to go directly to Section C.

## **B. Key Issues and Terminology in the E-Discovery Process**

At every stage of the e-discovery process, lawyers are asked to give advice to clients about issues that involve new concepts, and new terminology, that highlight key differences between the discovery of electronic documents and traditional paper-based files. At each stage, disputes may arise about those issues that require court resolution. As a result, to deal effectively and consistently with these issues, both lawyers and the judiciary need to become familiar with new concepts and related terminology in the area of e-discovery.

This section introduces some of the most important ones that arise at each stage of the e-discovery process.

The stages of the e-discovery process do not themselves differ from those involved in traditional hard copy discovery. They are:

- (a) **LOCATION** of potential document sources;
- (b) **PRESERVATION** of potentially relevant materials;
- (c) **REVIEW** of documents for relevance, privilege and other issues; and
- (d) **PRODUCTION** to other parties, for use in court proceedings.

---

<sup>3</sup> For a detailed glossary of frequently used terms, see The Sedona Conference® Glossary For E-Discovery And Digital Information Management. A Project of The Sedona Conference® Working Group on Electronic Document Retention and Production (WG1) RFP+ Group May, 2005; available on The Sedona Conference website ([www.thesedonaconference.org](http://www.thesedonaconference.org)).

Only by understanding the new concepts and terminology that come into play at each of these stages in the case of e-discovery, can lawyers and judges make informed decisions, avoid potential disputes in this area, or resolve them in a manner consistent with the Rules. This includes when and why it may make sense to seek or order production of electronic documents, and how to do so in a manner that remains cost effective to the parties.

### **(i) The Location of Electronic Documents**

The first question that arises is what must be located, within the existing Rules definition of “data and information in electronic form”?

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. It is also generally accepted that this definition includes many familiar types of electronic “documents,” such as e-mail, web pages, word processing files, and databases that are stored on computer.<sup>4</sup> However, both the definition and case law suggest that a broader range of electronic “data and information” may also be covered in some cases. The limitations on what may be covered are not to be found so much in technical distinctions, as they are in the familiar criteria of relevance.

The next obvious question is what computer systems the client has, or had at the relevant time, that may contain relevant data or information. Again, depending on the nature of the case, the answer may include enterprise systems or networks, as well as personal computers (desktops, laptops, and even hand-held devices), and even individual components and media relating to them, such as memory chips, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes.

The variety of hardware and media involved can pose problems for lawyers, clients and the courts. For example:

- some items may be in use by individual witnesses, others in storage in different areas or departments, and the documents may be in a wide variety of different electronic formats;
- copies of the same document may be stored in multiple locations in the course of normal operations: for example, an e-mail sent from one person to another on a networked system may be saved by each of the sender and recipient on their own computers, and further copies retained by the system for a variety of purposes;
- relevant electronic documents, even those created using systems that were once commonplace, may have become unreadable over time because of the unavailability or obsolescence of key software or hardware components;
- in some cases, the sheer volume of data can be enormous, both because of the expanding use of computer systems and their increasing storage capacity, and also because of the way they affect the behavior of people and organizations: for example, e-mail is not only replacing traditional paper-based communications such as letters and memoranda in many circumstances, it is also replacing many informal exchanges that in the past were not documented fully or at all, such as telephone calls and even casual conversations.

---

<sup>4</sup> THE SEDONA PRINCIPLES: Best Practices Recommendations & Principles for Addressing Electronic Document Production. A Project of The Sedona Conference<sup>®</sup> Working Group on Best Practices for Electronic Document Retention & Production, published January 2004.

These factors can all make the process of locating and assembling electronic documents for litigation purposes more difficult than for traditional paper-based materials. The involvement of clients' IT staff is often essential to ensure that the assembly process is complete and problem-free.

In order to ensure the completeness of searches, lawyers also need to understand some of the different sources of documents that may exist within a given organization's computer systems, and their different purposes. Here, discussion with IT staff or consultants is essential, and the use of correct terminology can anticipate problems and avoid mistakes. For example, electronic documents familiar both in personal and business usage - such as word processing, spreadsheet, database and e-mail documents - may be found in several different electronic locations and formats. A complete search should consider the following possible sources:

- “**Active data**” is data that is currently used by the parties in their day-to-day operations. This type of data is normally straightforward to identify and access using the current systems. However, because this data is in active use, significant issues may arise for lawyers and courts concerning the need to preserve the integrity of this data for litigation, to design and manage searches to avoid business disruption, and to separate relevant from irrelevant information.
- “**Archival data**,” on the other hand, is data organized and maintained for long-term storage and record keeping purposes. Some systems allow users to retrieve archival data directly, but others require special equipment or software, and the involvement of IT staff.<sup>5</sup>
- “**Backup data**” is similar to archival data, except that this term refers to an exact copy of system data, which serves as a source for recovery in the event of a system problem or disaster. Backup data is generally stored separately from active data, and is distinct from archival data both in the method and structure of storage that reflect its intended uses. It is generally not accessible to ordinary system users, and requires special (and sometimes expensive) intervention before it is “readable.”

Archival and backup data both constitute a set of electronic data and information collected for a particular purpose, and perhaps as at a moment in time. That purpose and timeframe may or may not be related to the litigation, and their relevance and completeness need to be assessed in that light.

Lawyers and the judiciary should also be aware that certain electronic sources, such as internet web-pages or database applications, may be under constant revision as new information is published on the site or added to the system. Unless these documents are located promptly, the available active copy may not reflect what the data actually looked like at the point in the past that is relevant to the litigation. Lawyers should be prepared to question their clients, to confirm which of the available versions are the best evidence for litigation purposes.

The documents most commonly requested and produced in litigation are those created by word processors, databases, spreadsheets, e-mail, and other familiar programs. These documents are routinely used and exchanged in business and private dealings. As noted above, these documents are normally quite easy to identify and locate. However, in discussions with IT staff involved, lawyers also need to be aware that many other, different kinds of “information and data” can exist in computer systems, in order to assess how and when they may be relevant. These may include less familiar kinds of documents, such as web-pages, browser history files that track a user's movements between web-sites and pages on the internet, cell-phone

---

<sup>5</sup> The Sedona Conference® Glossary For E-Discovery And Digital Information Management. A Project of The Sedona Conference® Working Group on Electronic Document Retention and Production (WG1) RFP+ Group May, 2005.

logs, and many other kinds of information stored on computer-based devices in their day-to-day operations. Most users may be completely unaware these documents even exist.

In addition, there may be hidden data or information associated or related to electronic documents that should be considered, particularly if there are issues of authorship or authenticity raised with respect to a document. Case law suggests that any data or information that can be readily compiled into viewable form, whether presented on the screen or printed on paper, is potentially within the definition of “document” under Rule 30.01 of the *Rules of Civil Procedure*. Again, some understanding of the concepts, as well as the terminology involved, is essential.

- “**Meta-data**” refers to electronic information that is recorded by the system about a particular document, concerning its format, and how, when, and by whom it was created, saved, assessed, or modified. For example, most word processing software records who created or modified a document, as well as the dates and times of document revisions. Most e-mail software records the dates and times e-mails are created, sent, opened, and saved as well as the names of the originator and all recipients, including those “blind copied.” This information may not be seen by users or appear in a print-out of the document in the ordinary course of business. However, meta-data is generally readily available, and can be extracted in searchable or printable form if it is relevant to litigation. Meta-data may be relevant directly to the litigation or it may be relevant to the authenticity and admissibility in evidence of the electronic documents with which it is associated, where this is disputed. Accordingly, its importance should not be underestimated.<sup>6</sup>
- “**Residual data**” refers to any information that remains stored on a computer system after a document has been deleted. The computer does not necessarily “wipe clean” the disk or memory space in which the file was stored, but merely “tags” it as re-usable by the system. The “deleted” data may not become truly unavailable until this space is re-used. Hence, deleted files or fragments of deleted files are often retrievable for some period of time after “deletion.” This can provide information about a document, and sometimes about changes made in successive revisions of a document, that would not otherwise be available. This kind of information is only recoverable using special “forensic” methods, and is unlikely to have significance in most litigation.
- “**Replicant data**” is created when a software program, such as a word processor, makes periodic back-up files of an open file (e.g. at five minute intervals) to facilitate retrieval of the document where there is a computer malfunction. Each time the program creates a new back-up file, the previous back-up file is deleted, or tagged for reuse.

Lawyers must understand the different kinds of electronic documents that may exist, and their characteristics, in order to assess whether and how they may be relevant, and where they may be found in a given case. Without some guidance from their lawyers on these issues, parties involved in litigation are unlikely to be able even to identify and locate the various electronic information and data that may have key relevance to their dispute.

## (ii) Preservation of Electronically Stored Documents

A party’s duty to preserve electronically stored documents that are relevant to contemplated or threatened litigation arises in the same way as for paper documents.

---

<sup>6</sup> The Sedona Conference® Glossary For E-Discovery And Digital Information Management. A Project of The Sedona Conference® Working Group on Electronic Document Retention and Production (WG1) RFP+ Group May, 2005.

However, the discussion and terminology reviewed above highlights some special problems that can arise in the preservation of electronic documents, and also suggests how they can be addressed. Specific guidance is offered in Section C below, but the following are some examples of practical problems that arise from the lack of such understanding, and of the solutions that may often be available.

- Electronic documents or media containing them may be considered obsolete by the client in terms of its current business systems, but may nevertheless be recoverable to a readable form by specialized forensic methods. The costs involved, at least for many of the most commonly used methods, have declined to a point that may be cost effective in an increasing range of litigation.
- Relevant meta-data may exist at the time an electronic document or source is located, but may be altered or lost simply in the process of making a copy of the relevant electronic files for litigation purposes. This again is avoidable, as relatively affordable techniques exist, either to make “forensic copies” or “mirror images” that are specifically designed to preserve the integrity of the meta-data, or to capture the relevant meta-data from the original source documents before they are copied.
- Preserving web-site files in electronic form, rather than simply printing them up at a point in time, may enable a party, at minimal cost, to recreate the website electronically in a courtroom, in order to demonstrate dynamically any relevant links, relationships, and special features that characterized the site at the time the litigation arose.
- Formal document retention policies are a relatively recent development, and even today may not be standard except in the very largest and most sophisticated organizations. Moreover, sound business reasons may exist for practices that result in the destruction of relevant electronic documents: for example, routine deletion or omission to back-up e-mail to maintain storage space. For these reasons, early discussion with IT staff is often necessary to prevent continued deletion after litigation is threatened or commenced.

These examples illustrate the point that, in order to understand how to comply with or enforce the obligation to preserve electronic data and information for litigation, parties, lawyers and the courts first need to understand the characteristics of electronic documents and the concepts and terminology of e-discovery discussed above.

### **(iii) Electronic Document Review**

The preceding discussion of the ways electronic documents differ from paper also affects the approaches to the review of available electronic materials for litigation purposes.

Review of electronic documents is essential, first, to separate relevant materials, which should be produced, from irrelevant material, which should not. Over-production of irrelevant electronic documents may be just as damaging to clients’ interests and the litigation process as incomplete production.

However, the sheer volume and particular characteristics of electronic documents may be a significant barrier to effective review, for a number of reasons:

- Many institutions and businesses save a copy of their entire system onto back-up tapes periodically, and some retain them for long periods of time. Computer back-up tapes can store huge amounts of data, which may be organized for purposes of disaster recovery, rather than normal usage. It often needs to be converted back to readable form, before it can be searched or printed out to determine relevance. The

volume and organization of archive and backup data, and costs of conversion, can be significant barriers to production, especially as restoration may require processing a complete set of back-up tapes together.

- Depending upon the institution's retention policies, the resulting set of documents (although complete and accurate for the purposes for which they were stored) may be incomplete or may not fully reflect the status of the same documents at the time relevant to the litigation.
- The document set may also contain multiple duplicates. Electronic documents are easily duplicated and, as noted above, copies of the same document may be stored in multiple locations in the course of normal operations. Consequently, although a user may have deleted his/her own copy, others persist in other locations, often without the user's knowledge.
- Earlier versions (including drafts) or later versions may still be retained. Unless clearly marked – or better yet, unless the relevant meta-data has been preserved - it may be impossible to know which version is earlier or later, and which version is relevant to the timeframes and issues raised in the litigation.
- Since even meta-data could, in certain cases, contain or reveal privileged, secret, or other sensitive information, an organization may determine that it too must be separately reviewed before the documents are produced.

Once the files are collected in readable form, manually searching for and retrieving specific files may be cumbersome, time-consuming and prohibitively expensive. Depending on the documents and the technology used, however, automated search tools may offer solutions. E-discovery has been greatly facilitated by new technologies that permit some kinds of electronically created documents to be converted from one digital form into another, in large volumes, often at minimal cost. This means that in some cases the practicing lawyer and client may no longer face prohibitive cost and technology barriers to the review and searching of electronic documents, particularly with respect to many common forms of electronic documents, such as e-mail.

In some cases, however, even the available electronic tools may not permit complete review for production in litigation on a cost-effective or timely basis. Lawyers and the judiciary in such cases need to seek agreements, or arrive at terms for court orders, that target the most relevant data and information.

#### **(iv) Production of Documents in Electronic Form**

The question lawyers are increasingly asked to advise on (and courts may be asked to adjudicate) is whether parties may simply print out electronic data such as e-mails, or whether they are obliged to produce them to the opposing party in electronic form. The answer in any given case may involve a balance of competing considerations.<sup>7</sup>

In order to maximize the benefits of e-discovery, the courts and the profession need to gain experience with respect to such issues as: what circumstances call for electronic production as opposed to paper production;

---

<sup>7</sup> For example, many electronic documents involve more than mere printable text. In a database application, individual pieces of information may be meaningless, unless they are produced within their context or environment, and the ability to manipulate relevant information using the original software application in which it was created may bring added benefits. However, a database may often contain irrelevant, confidential, and even privileged information, together with the relevant information, or the software application may not be available commercially, or at all, to third parties. In such cases, standard or custom "reports" displaying the relevant information with the context in a readable form might be generated, without producing the entire system, and may be sufficient.

how the cost of production should be fairly allocated; how to ensure that electronically produced documents are compatible with courtroom technology to facilitate production at trial; how to provide for the redaction of privileged and irrelevant material in electronic form; and how to ensure appropriate retention of electronic records.

These issues are very much affected by the availability of new technology, and its increasing use by lawyers and courts. Most litigation support software provides for exporting production sets in formats that allow them to be imported by a recipient party into the litigation support tool of their choice. Many of these tools are designed to produce properly redacted versions of documents<sup>8</sup>, to permit the creation of special fields for production of relevant meta-data, and to allow the user to select which fields will be exported.

Similarly, large volumes of hard copy documents can be scanned as image files, and exchanged on CDs or via web-based software, often at less cost than would be involved in producing a similar number of photocopy sets. This is especially important in multi-party litigation, and where parties have the opportunity to share the costs of scanning. With the assistance of available software tools, electronically scanned documents can be much easier and more efficient to store, organize, manage and search, than equivalent volumes of paper documents. These developments are rapidly reducing cost and technological barriers to high-volume document cases, even where the client's source documents exist in paper form.

However, the use of these new tools and methods is still limited, and sometimes inconsistent, among lawyers and the judiciary. These Guidelines are intended to promote the efficient use of technology in the discovery process. The control of escalating costs, together with increased effectiveness for lawyers and parties advancing their case through the discovery process, is an important part of the rationale behind these Guidelines.

## **C. Principles that should Guide the E-Discovery Process**

### **(i) Discovery of Electronic Documents (“E-Discovery”)**

Principle 1: ***Electronic documents containing relevant data and information are discoverable pursuant to Rule 30.***

*Commentary:* As soon as litigation is contemplated or threatened, it is essential for parties and their counsel to go beyond paper file searching, and consider what electronic data and information exists that they may need to produce. Parties must take reasonable steps to locate and preserve electronic documents containing data and information that can reasonably be expected to be relevant to litigation. Further, parties should consider what relevant electronic documents other parties may have, that they may want to request be preserved for production in the course of the litigation.

Principle 2: ***The obligations of the parties with respect to e-discovery are subject to balancing, and may vary with (i) the cost, burden and delay that may be imposed on parties; (ii) the nature and scope of the litigation, the importance of the issues, and the amounts at stake; and (iii) the***

---

<sup>8</sup> Counsel using such tools should ensure that redactions are permanently embedded in the production copy of the document, and cannot be electronically “undone”. Counsel should also ensure that, if a full-text or OCR version of the documents is also being produced, this version, as well as the image, should be redacted.

***relevance of the available electronic documents, and their importance to the court's adjudication in a given case.***

*Commentary:* This principle is consistent with Rule 1.04(1), and the objective of securing the just, most expeditious, and least expensive disposition of litigation on its merits.

Even where there has been complete production in paper form, electronic versions of the same documents may contain relevant meta-data that may not appear in a printout or scanned version of the document. Meta-data may be directly relevant in the litigation, or it may be relevant where there is an issue as to the authorship or authenticity of a document. In such situations, it may also be necessary to produce the relevant meta-data in some form. Parties should consider whether it may be preferable to produce the entire document, including the meta-data, in electronic form.<sup>9</sup>

The questions to be considered in determining whether to require the use of forensic techniques to recover back-up or obsolete sources include not only the costs involved, and the potential amount, usability, reliability and relevance of the information to be obtained, but also:

- whether the party believes that the materials available from active electronic and paper sources are reasonably complete;
- whether the party has rules for printing up or retaining important documents in electronic form, and whether they are monitored for compliance; and
- the availability and completeness of the back-up or obsolete sources.

Parties should use the most cost-effective methods to locate, preserve, review and produce electronic documents. Electronic documents may be easier to search than printed or scanned copies, and therefore more effective in litigation, and production of documents in electronic form may be more cost-effective than print production.

The costs to be considered may, where appropriate, include the costs of counsel and any necessary consultants, hardware, software or other facilities or services required (i) to recover or make electronic documents available in a readable form; (ii) to search documents in various formats to identify relevant material, and separate irrelevant material; (iii) to review the relevant documents for privilege; (iv) to produce the documents to other parties;

---

<sup>9</sup> An example of a case where resort to back-up tapes was ordered by the court is in the U.S. decision of *Zubulake v. UBS Warburg LLC*, 2003 W.L. 21087884 (S.D.N.Y. May 13, 2003), an action claiming gender discrimination and illegal retaliation, where a request for an order compelling UBS to produce various e-mails now existing only on back-up tapes and other archived media was before the court. Despite the fact that UBS had already produced approximately 100 pages of e-mails, Zubulake believed it had more based on the fact that she herself had produced approximately 450 pages of e-mails. The court determined that UBS should provide tangible evidence of what the backup tapes might have to offer in the form of a sample. UBS was therefore ordered to produce responsive e-mails from any five back-up tapes selected by the plaintiff. UBS was also required to prepare an affidavit detailing the results of its search, as well as the time and money spent. Following the production of relevant e-mails taken from the sample back-up tapes, UBS was ordered to restore its back-up tapes and produce responsive e-mails from these tapes. The case suggests that, where a party on proper evidence convinces a court that documents have not been produced and that such documents are likely stored on a computer hard drive or other electronic storage medium, such as back-up tapes, but the party in possession of the computer asserts it has printed or produced all that it has, then the only solution would be to allow inspection of the storage medium itself or restoration of the documents from back-up tapes.

and (v) to enter them in evidence through discovery or at trial. Consideration of the burden and delay involved should also include the likelihood of disputes at any stage of the process.

Consideration of the relevance and importance of the available electronic documents should include their admissibility and mode of proof as evidence.

Principle 3: ***In most cases, the primary source of electronic documents should be the parties' active data, and any other information that was stored in a manner that anticipated future business use, and that still permits efficient searching and retrieval.***

*Commentary:* The scope of the searches required for relevant electronic data and documents must be reasonable. It is neither reasonable nor feasible to require that litigants immediately or always canvass all potential sources of electronic documents in the course of locating, preserving, and producing them in the discovery process.<sup>10</sup> Some sources may contain largely duplicate documents or redundant information and data. Others may contain few if any relevant documents, together with massive amounts of data and information that is not relevant to the litigation.

This principle is based on the premise that, for most litigation, the most relevant data and information will be that which is available to or viewed by the computer users, and that which is exchanged between parties, in the ordinary course of business. This is normally the active data, but the principle also includes archival data that is still readily accessible and not obsolete. Litigants must exercise judgment, based on reasonable inquiry in good faith, to identify such active and current archival data locations that may be subject to e-discovery.

However, if a party is aware (or reasonably should be aware) that specific, relevant data or information can only be obtained from a source other than the active and current archival data sources, then that source should at least be preserved and listed appropriately in the party's Affidavit or documents for possible production, absent agreement of the parties or order of the Court.

Principle 4: ***A responding party should not be required to search for, review or produce documents that are deleted or hidden, or residual data such as fragmented or overwritten files, absent agreement or a court order based on demonstrated need and relevance.***

*Commentary:* Unless residual or replicant data, or other material that is not accessible except through forensic means, is known or should reasonably be known to be available and relevant, it need not be preserved or produced.

If such data is considered relevant, parties should request its preservation as early as possible, in order to avoid inadvertent deletion or claims of deliberate destruction.

---

<sup>10</sup> In *Dulong v. Consumer Packaging Inc.*, (2000) O.J. 161 (Q.L.), (January 21, 2000, Ontario Master), the court held that a broad request that the corporate defendant search its entire computer system for e-mail relating to matters in issue in the litigation was properly refused on the grounds that such an undertaking would, "having regard to the extent of the defendant's business operations, be such a massive undertaking as to be oppressive".

## (ii) Preservation of Electronic Documents

Principle 5: *As soon as litigation is contemplated or threatened, parties should immediately take reasonable and good faith steps to preserve relevant electronic documents. However, it is unreasonable to expect parties to take every conceivable step to preserve all documents that may be potentially relevant.*

*Commentary:* The obligation to preserve relevant electronic documents applies to both parties. Counsel should advise clients with respect to this obligation at the earliest possible time, including the steps that may be prudent or required to implement a “litigation hold”.

These may, in appropriate cases, include steps to:

- (i) collect all relevant document retention, back-up, archiving, and destruction policies;
- (ii) issue appropriate instructions to all staff, or at least to relevant staff, to cease or suspend personal activities and practices that could result in the destruction or modification of relevant electronic documents, such as the deletion of e-mailbox entries or archives;
- (iii) create litigation copies of potentially relevant active data sources, for example by means of electronic backup or forensic copying of the documents, so as to preserve potentially relevant meta-data; and
- (iv) cease or suspend the overwriting of back-up tapes, and other document retention practices that could result in the destruction or modification of relevant electronic documents in the ordinary course of business.

Where applicable, electronic document retention policies should be shared so that both parties are aware of what electronic documents may exist and what may no longer be accessible. This may include disclosing the procedure and cycle for electronic backup for each system and/or any procedure for archiving electronic documents. Parties should also consider sharing any available lists of electronic records stored off-site or off-system. Sharing this information will assist both parties in identifying the documents that need to be preserved for litigation, and the steps required to do so.

Principle 6: *Parties should place each other on notice with respect to preserving electronic documents as early in the process as possible, as electronic documents may be lost in the ordinary course of business.*

*Commentary:* Where parties or counsel anticipate that specific electronic documents do or may exist that are relevant to litigation and that are liable to be deleted or modified in the ordinary course of business, they should immediately notify the client or opposing party of that fact, and request that appropriate steps be taken to preserve the documents.

Counsel should also consider, as early as possible, whether third parties may be in possession of relevant electronic data, and the steps required for its preservation.

Principle 7: ***Parties should discuss the need to preserve or produce meta-data as early as possible. If a party considers meta-data relevant, it should notify the other party immediately.***

*Commentary:* Depending on the circumstances of the case, particular meta-data may be critical or it may be completely irrelevant. The relevance of meta-data warrants particular consideration, however, because (i) it is readily alterable, either intentionally or inadvertently, for example if non-forensic “copies” of electronic documents are made for litigation purposes; (ii) it may be relevant either directly, to an issue in the litigation, or to any dispute about the authenticity, admissibility and proof of relevant electronic documents with which it is associated; and (iii) sometimes, meta-data can lead to inaccurate conclusions, for example, in a situation where a document is created from a standard “form” which identifies the “author” who created the form, but not the person who drafted the actual or ultimate document produced from it.

The meta-data associated with e-mail documents is relevant, and even necessary to list the documents accurately in an Affidavit of Documents. Parties should ordinarily expect that this type of meta-data be preserved and produced in litigation. For many other types of meta-data, however, this kind of data is technical in nature, and forensic techniques are required for its extraction. The relevance of this type of meta-data is usually confined to particular kinds of litigation, or particular documents: for example, the history of prior revisions to documents may be broadly relevant in a fraud case, or in the case of a particular contract or other document in issue. It is seldom if ever required for routine correspondence to prove any point in contention.

In general, it is only where the producing party knows or should reasonably know that particular meta-data is relevant to the dispute, that it should be preserved. However, litigants need to scrutinize claims and defences before determining how to handle meta-data. Organizations should not automatically discount the potential benefits of retaining meta-data to ensure the documents are authentic and to preclude the fraudulent creation of evidence.<sup>11</sup> Parties and their counsel should consider at the outset of litigation the need to preserve and produce meta-data, and be prepared to discuss this with opposing parties and counsel.

### **(iii) Pre-Discovery Discussions between Counsel: Defining the Scope of E-Discovery Obligations**

Principle 8: ***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.***

---

<sup>11</sup> Notwithstanding this, the routine preservation of meta-data may be beneficial in a number of ways. First, it avoids any risk of allegations of inadvertent or deliberate modification of evidence. Second, simply preserving documents in their native electronic format usually preserves the associated meta-data, without incurring any additional steps or costs. Third, the failure to preserve and produce metadata may deprive the producing party of the opportunity to later prove or contest the authenticity of the document, if the meta-data would be material to that determination. Finally, systematic removal or deletion of some meta-data may involve significant additional costs that are not justified by any tangible benefit, while the cost of preserving it in many cases may be practically nil.

*Commentary:* By early discussion of e-discovery issues, litigants can identify and attempt to resolve disputes before they create collateral litigation. The issues commonly requiring early discussion include (i) the relevant time period, (ii) the identity of individuals likely to have created or received relevant electronic documents in the period; (iii) which computer systems or media existed and are available relating to that period, (iv) which electronic documents can and should be preserved; (v) which electronic documents can be made accessible and searched on a cost effective basis; (vi) what searches should be conducted to identify relevant materials, including the “key words” to be used to perform these searches; and (vii) in what form should the relevant materials be produced. Particular cases may, however, raise additional or different issues.

Creating checklists of the key issues to consider during an e-discovery conference can guide the parties and minimize the likelihood of disputes or inadvertent alteration or destruction of electronic documents. Counsel should also be prepared to discuss e-discovery issues with the court at an early stage, whenever case management or other rules provide an opportunity to do so before disputes arise.

Parties will benefit if counsel are able to agree on an e-discovery plan. Since electronic documents are not tangible, there are options for delivering the data. These will need to be discussed by the parties and possibly the court. Counsel need to decide how electronic documents should be produced, and reach agreements as to format, document numbering and other important housekeeping issues. Counsel may also wish to address substantive issues of admissibility, proof, redaction and the removal of privileged material.

The requesting party should prepare a detailed specification of what information is being sought, from what sources, and how the information should be formatted and delivered. Where “native format” information is being sought, the requesting party should identify the properties that must be preserved. To reduce the possibility of miscommunication, counsel may want to exchange sample data, or exchange limited amounts of data, to assure that both parties are receiving what they anticipated before the costs of full production are incurred.

The producing party should be in a position to produce an affidavit or other documentation detailing the data acquisition process and describing the pre-production processing of the data. For example, a party may decide to pre-screen e-mail to remove information that is personal, non-responsive, or duplicative. Although such a process can be entirely appropriate, requesting parties need to know what standards were used for the pre-screening process. For example, are identical e-mails delivered to different mailboxes considered duplicates?<sup>12</sup>

Parties and counsel should also provide early notice of any problems reasonably anticipated to arise in connection with their respective rights and obligations, or the process relating to e-discovery. This should include (i) the identification of potentially relevant data that is likely to be destroyed or altered in the normal course of operations or pursuant to the party’s document retention policy, (ii) any limitations on the search efforts they propose to undertake, (iii) any requests from the opposing party or counsel they consider to be burdensome, oppressive, or unreasonably expensive, and (iv) their position with respect to any proposed change to the normal allocation of costs.

---

<sup>12</sup> “A Practical Guide to Electronic Discovery in Construction Disputes”, Howard W. Ashcraft, Jr., Hanson, Bridgett, Marcus, Vlahos & Rudy, San Francisco, U.S.A.

Relevant electronic documents or sources that are known to be no longer available should be listed in Schedule C to the party's Affidavit of Documents.

Principle 9: ***The scope of e-discovery should be defined by parties and their counsel before commencing oral examinations for discovery. This can best be achieved if parties' requests for preservation of electronic documents, and pre-discovery meetings between counsel, are as specific as possible in identifying what is requested, what is being produced, and what is not being produced, and the reasons for any refusals.***

*Commentary:* Unnecessary controversy over peripheral discovery issues can often be avoided at the outset by discussion between the parties regarding the potential scope and related costs of preserving and producing relevant electronic documents.

In many United States jurisdictions, issues relating to the scope of e-discovery are managed through a process of written requests for production, and responses, before pre-trial examinations commence. This has many benefits, and can avoid many problems, if the requests and responses are sufficiently detailed and specific. These same benefits can be obtained within Ontario practice, if the issues are addressed in similar detail through early requests for preservation of electronic documents, and pre-discovery discussions between counsel, before commencing oral examination for discovery.

These requests and discussions should avoid boilerplate approaches, which often seek all e-mail, databases, word processing files, or whatever other electronic documents the requesting party can describe by category. Instead, counsel should target particular electronic sources, documents or timeframes that they contend are truly important to resolve the case. By identifying particular relevant electronic documents, and understanding when and why printed or scanned versions are inadequate in the particular case, parties can avoid the sort of blanket, burdensome requests for electronic documents that invite blanket objections and judicial intervention.

Parties should also identify the form in which they wish electronic documents to be produced.

Parties should generally not require production of hardware media such as computer hard drives. These are media on which data is stored, and may be thought of as an electronic filing cabinet. However, in exceptional circumstances, parties may need to inspect hardware media. For example, where a party has reasonable grounds to believe that documents (or meta-data associated with documents) have not been produced, and are likely still stored on a computer hard drive or other electronic storage medium, but this is disputed, then the only solution may be inspection of the storage medium itself, with proper safeguards.<sup>13</sup>

Principle 10: ***A party may satisfy its obligation to produce relevant electronic documents in good faith by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify the documents that are most likely to contain relevant data or information.***

---

<sup>13</sup> This type of relief, if opposed and not consented to, is normally available only by order under s. 101 of the *Courts of Justice Act*, as a form of injunction akin to an Anton Pillar order.

*Commentary:* Particularly where searches for relevant electronic documents must be undertaken on large computer systems, containing vast amounts of information, including materials that are likely to be irrelevant, it may be impractical or prohibitively expensive to review all that information for relevance and privilege. In such circumstances, it is reasonable for parties to use electronic techniques to search within electronic document sources, in collecting the materials that will be subject to detailed review for relevance and privilege. The objective should be to identify a subset or subsets of the available electronic documents for detailed review, that are most likely to be relevant.

Where possible, parties and counsel should agree in advance on the search methods, and selection criteria or search terms, that will be used. Absent such agreement, however, parties should record and be prepared to disclose any limits on the searches they have undertaken, and to outline the scope of what they are producing, and what potential sources or documents have not been searched.

#### **(iv) Production of Electronic Documents**

Principle 11: *Parties should agree early in the litigation process on the format in which electronic documents will be produced. Such documents may be producible in electronic form where this would (i) provide more complete relevant information, (ii) facilitate access to the information in the document, by means of electronic techniques to review, search, or otherwise use the documents in the litigation process, (iii) minimize the costs to the producing party, or (iv) preserve the integrity and security of the data.*

*Commentary:* Parties must produce a document in electronic form if, for any reason related to the litigation, it is not sufficient to produce a printout or scanned version of the document.

Parties and their counsel should consider agreeing to the production of documents electronically, rather than in print, where this can result in savings in costs to the parties.

Production of voluminous documentation in a form that does not provide meaningful access should be avoided. Electronic documents should not be converted to another form for production purposes, including creating printouts or scanned versions, if this has the effect of denying meaningful access to those documents. Where one party has documents in a searchable form, such as an electronic database, the searchable format should ordinarily be produced to other parties where possible. However, the use of printouts or reports may be justified in the case of documents containing both relevant and irrelevant information, if the relevant information cannot be segregated in a searchable format.

In cases involving voluminous documentation, where digitizing documents may be appropriate or where documents need to be organized in a common, indexed fashion, parties should attempt to agree upon a protocol to address these issues, and for the sharing of the costs involved. However, the format in which this is done should be carefully controlled to avoid loss of privilege or the production of irrelevant materials. As noted, most litigation support software provides for exporting production sets, in formats that allow them to be imported by a recipient party into the litigation support tool of their choice, and many of these tools are designed to enable counsel to produce only the relevant fields, together with properly redacted images of the documents.

## (v) Privilege

Principle 12: ***Where appropriate during the discovery process, parties should agree to measures to protect privileges and other objections to production of electronic documents.***

*Commentary:* E-discovery does, in some circumstances, involve a heightened or special risk of inadvertent or unintended disclosure of privileged information. Examples cited in the literature and anecdotally include:

- production of large volumes of electronic documents, for electronic searching, such as a computer hard-drive or back-up tape; and
- an Anton Pillar injunction, search warrant, or other order for immediate production of documents to an adverse party, without prior review for privilege.

Again, however, as these examples suggest, the problems of inadvertent or unintended disclosure of privileged information are not necessarily different in kind for e-discovery as opposed to production of hard copies. Rather, the risk of occurrence may be greater in an e-discovery context, simply due to the volume of information involved, or to the difficulty and potential delay in identifying the privileged subject matter (where for example it takes the form of privileged meta-data or attachments associated with an otherwise non-privileged document.) That increased risk is significant, because the consequences of inadvertent or unintended disclosure are serious, potentially for both parties, including disqualification of counsel.

Counsel should discuss how to protect privileged documents at the outset of litigation.

Counsel should also recognize that, given a large volume of electronic documents, review for privilege will take time. Counsel should agree on measures to prioritize review, and streamline production of non-privileged material, without loss of privilege.

Special issues may arise with any request to inspect hardware media such as computer hard drives. Parties should consider how to guard against any release of proprietary, confidential information and protected personal data if such media are to be inspected.

## (vi) Costs

Principle 13: ***In general, consistent with the rules regarding production of paper documents, pending any final disposition of the proceeding, the interim costs of preservation, retrieval, review, and production of electronic documents will be borne by the party producing them. The other party will, similarly, be required to incur the cost of making a copy, for its own use, of the resulting productions. However, in special circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by agreement or court order.***

*Commentary:* In Ontario, the traditional presumption is that the producing party is responsible for its own costs of meeting its obligations in the discovery process. However, once the documents are

ready to be produced, the opposing party is responsible for the immediate costs of the production of documents to them, such as copying, binding and delivery costs. Any other cost-shifting occurs at the end of the litigation, at which time the unsuccessful party may be required to contribute, in whole or in part, towards the costs (fees and disbursements) of the successful party. In the United States, to the contrary, the litigation process usually does not involve cost-shifting at the end of the litigation, and places more emphasis on interlocutory cost-shifting. Hence, case law and commentary dealing with costs in those jurisdictions should be applied with caution, if at all, in Ontario.

E-discovery may involve significant internal client costs, as well as counsel fees and disbursements for out-sourced services, at both the stage of locating and reviewing electronic documents and at the production stage. As such, there may be a need for the costs rules to be clarified so that internal discovery costs may be regarded as a recoverable disbursement in appropriate cases.

As the e-discovery costs borne initially by producing parties may be significant, such parties may wish to adopt strategies so as to control the costs of e-discovery. For example, a producing party may wish to limit, either through negotiation, appropriate admissions, or motions, the extent and scope of their e-discovery obligations. They may also wish to consider whether the costs should be partially or completely shifted to the requesting party. As well, a producing party may wish to serve on the requesting party a Rule 49 Offer to Settle, or to seek security for costs, to enhance its chances of recovery if it is ultimately successful in the proceeding.

However, given the potential for interim costs awards in an e-discovery context, the parties seeking production of electronic documents should also carefully consider the cost-implications of these claims. At a minimum, if they are ultimately unsuccessful, these parties may then be responsible for a significant portion of these e-discovery costs.

## **Conclusion: The Need for Ongoing Refinement of these Guidelines**

As noted in the introduction, it is intended that these Guidelines will be developed over time as technology develops, and as the bench and bar gain experience with e-discovery in practice. It is expected that refinements to the Guidelines together with reference material will be available through the internet in due course.

This process of development will be ongoing. Members of the bar and interested groups are expected to take a leadership role. Input from practice groups involved in personal injury, commercial, intellectual property and other specialized types of litigation, will be particularly important. The judiciary is also encouraged to participate, for example, by providing additional sample orders and agreements that would not otherwise be widely reported or available, to illustrate and flesh out specific issues and practices.

## **APPENDIX A**

### **Sedona Principles for Electronic Discovery**

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.
2. When balancing the cost, burden and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state-law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.
3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.
4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.
5. The obligation to preserve electronic data and documents requires reasonable and good-faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.
6. Responding parties are best situated to evaluate the procedures, methodologies and technologies appropriate for preserving and producing their own electronic data and documents.
7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.
8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden and disruption of retrieving and processing the data from such sources.
9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review or produce deleted, shadowed, fragmented or residual data or documents.
10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.
11. A responding party may satisfy its good-faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching or the use of selection criteria, to identify data most likely to contain responsive information.
12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.
14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.