Table of Contents

Making and Responding to Requests for Electronic Discovery

"More money is probably spent litigating electronic discovery problems than in litigating class actions…this is part of potentially every case in the 21st century".[1]

Ken Withers, Senior Education Attorney at the
Washington-based Federal Judicial Center

Overview: Why You Need to Understand the Process of Electronic Discovery

It is often said that cases are more often won or lost at discovery. Electronic evidence has proven vital in determining the outcome in cases involving allegations of sexual harassment, disputes involving trade secrets, copyright infringement and insider trading. E-mail, chatroom transcripts, databases, spreadsheets, web browser history files, and information derived from system backup tapes are replacing conventional paper documents. Evidence has begun to take a new form as we have seen in the Microsoft anti-trust litigation,[2] the investigation of President Clinton by Judge Starr,[3] Ratheon Corporation's lawsuit against its own employees for libel,[4] and even in routine divorce cases. A sole e-mail from an in-house attorney at Arthur Anderson advising a partner to edit an internal memo about Enron Corp.'s financial disclosure helped to convict the accounting firm of obstruction of justice.

[1] Ameet Sachdev, *"E-mails become Trial for Courts: Costly Electronic Discovery – Part of Potentially Every Case in the 21st Century"*, Chicago Tribune, online edition, April 10, 2005

[2] *United States* v. *Microsoft Corp.*, Civil Action 98-1232 (TPJ) (D.C.D.C. 12 November 1999) (Findings of Fact) – see footnote cited in article entitled "*Electronic Disclosure and Discovery in Civil Litigation"* by Kenneth J. Withers (available on-line at http://www.kenwithers.com/articles/bileta/elecdisc.htm dated September 16, 2003)

[3] Kenneth T. Starr, "*Referral to the United States House of Representatives*" (o September 1998) HTTP://icreport.loc.gov/icreport/1.htm

[4] Adriana Estes and Todd Wallack, "*Ratheon case sparks showdown over internet privacy*" Boston Herald, 4 March 1999 at 001 – see footnote 4 in article by Kenneth Withers, "Electronic Disclosure and Discovery in Civil Litigation" (available on-line at http://www.kenwithers.com/articles/bileta/elecdis.htm dated September 16, 2003)

Today, the amount of electronic information stored at large corporations and the government, is staggering. Consider this estimate as explained by an Exxon Mobil lawyer: Exxon Mobil stores 800 terabytes of information, which equates to 400 billion typewritten pages[5]. It seems that if you are ignoring electronic evidence as a litigation lawyer in your discovery practices, you are missing out– it is equivalent to only reviewing 3 out of 10 file drawers of potentially relevant and discoverable information.

The Importance of Understanding e-Discovery

There are numerous reasons why it is important to understand the e-Discovery process. For the party asking the questions, you must be able to respond to objections relating to privacy and confidentiality issues, fishing expedition claims or complaints of overly broad requests. You will also need to understand when it is appropriate to require production of the metadata or hidden data, as requests for this information are not suitable or relevant in all cases. On the other hand, for the parties subject to the production request, you must understand e-Discovery in order to comply with discovery requests and to oppose or defend objectionable requests or overly broad requests. You must be able to convince a court that your objections are supportable in that they are based on legal and/or technological grounds. To successfully argue that a request is unduly burdensome or overly broad, counsel will be required to be familiar with both active and archived computer files, the capability of searching and retrieving the requested information (with respect to their client's computer systems) and the total cost associated with production and the requested retrievals, for example, of archived files.

[5] Ameet Sachdev, *"E-mails become Trial for Courts: Costly Electronic Discovery – Part of Potentially Every Case in the 21st Century"*, Chicago Tribune, online edition, April 10, 2005

Among the most common difficulties or sources of dispute with discovery of electronic data are:

(i) the location and volume of potentially relevant electronic information;

(ii) preservation of data subject to discovery;

(iii) scope of discovery;

(iv) format of production of electronic documents and, in particular, e-mail;

(v) the protection of privileged data;

(vi) the need to produce or look for deleted information;

(vii) the need to resort to backup tapes (including archives and legacy data to identify and/or retrieve potentially relevant information);

(viii) procedures for an on-site inspection; and

(ix) when expert assistance is required.

These issues are all relevant to making and responding to requests for production of electronic documents. This paper will be divided into two parts: the first part will provide an overview of the predominant challenges associated with e-Discovery demands and responses. The second part will provide useful tips to deal with the most common sources of dispute with discovery of electronic data.

Part I: Problems with e-Discovery

1. Volume

Most of the problems in the search for relevant electronic records are the same as for paper records, with one important difference: the number of individuals who must conduct searches and the quantity of records is significantly increased by the requirement to do electronic searches. E-mails and attachments are copied and forwarded to a much larger number of people than was previously done with paper communications. This practice significantly increases the

number of individuals who have to search for records and significantly increases the quantity of documents that have to be reviewed for relevance, privilege, confidentiality and, in the case of government institutions, public interest immunity. When searching for specific information on a database, hard-drive, server or other form of electronic storage, the task of finding this information amidst the mass of documents often becomes the proverbial needle in a haystack.

2. Wide Distribution of Data Sources

In addition to sheer volume, it is important to consider the dilemmas arising from defining a request for production. For instance, in litigation against the Government, the greatest and most common difficulties arise in identifying what ministries or departments may have information relevant to the dispute. For example, government staff did not call their documents "Walkerton" before the tragedy in Walkerton happened. Their subject areas may have related to numerous topics. It is not uncommon for different ministries or different departments within one organization to address aspects of the same problem from their different perspectives, totally unaware that other ministries also have an interest in an aspect of the issue of the problem. This poses a significant problem in litigation in locating potentially relevant records, whether they are electronic or paper. The defendant must, to some extent, rely on the plaintiff's characterization of the problem or issues as one relating to health or to the environment, etc. For example, if the plaintiff's claims relate to an alleged failure to provide adequate medical care, the logical place to look for relevant records is the Ministry of Health. It may not occur to those handling the litigation that several other ministries may have relevant documentation addressing the same issues from the perspective of education, the environment, or social services. Identifying where to look for relevant documents is a major issue in e-Discovery. On the other side, there are challenges to fulfilling e-Discovery requests when many different people or departments will

have created or dealt with the information sought. For instance, many executives store data directly (knowingly or unknowingly) on their office hard drives, or in remote media such as home computers, laptops and palm computers. This information may be more useful than material stored in network files, or it may be the only record of data that has otherwise been deleted because of document retention policies.

3. Lack of Planning or Proper Issue Identification

A computer search using vague and general search terms will necessarily turn up numerous irrelevant documents. Even terms that, to an outsider appear very specific, may produce a large quantity of irrelevant records. For example, in many companies or government departments, a computer search for "KPMG" (the forensic auditing firm) will undoubtedly produce records relating to many different matters unrelated to the matter that is the subject of litigation.

4. Overbroad Requests for Production

Where a request is overbroad, an objection is likely to ensue. In *Northwest Mettech Corp. v. Metcon Services Ltd.*, the court considered a request for production of computer hard drives containing Autocad drawings. Northwest brought an action against a former employee (who had moved to Metcon) for breach of confidentially and alleged that the former employee had appropriated confidential information belonging to Northwest concerning the design of a patented invention. The defence advanced was that the former employee had developed the invention designed prior to joining Northwest and the patent belonged to him and his subsequent employer, Metcon.

Northwest sought the production of documents including computer files and draft patent applications. In opposing the request for production of the hard drive itself, the defendants argued that they had enclosed all relevant documents including all relevant documents in electronic form resident on the former employee's computer hard drive. Evidence was also adduced before the court that the hard drive at issue no longer existed as the computer at issue had been sold at a garage sale. (Some of the files from the old hard drive were, however, transferred to a new computer, before the old computer was sold.) The respondents successfully argued that other data which is resident on the hard drive (of the new computer) was confidential and not relevant to the action. In making the determination that Northwest was not entitled to production of the hard drive, the court noted that:

> As I understand it, the computer hard drive is simply a medium on which data is stored on a semi-permanent basis in the form of electronic impulses. It may be thought of as an electronic filing cabinet which contains electronic files, each of which in turn contains electronic documents. The defendants are obliged to list all relevant documents of whatever form (including electronic documents resident on computer hard drives). In my view they are not required to list the entire contents nor are they required to produce their entire electronic filing cabinet anymore than a party is required to list or to produce the complete contents of its steel filing cabinets which house documents which are in paper format. In my view, the plaintiff has not shown any proper basis to require production of the actual hard drive. The plaintiff is entitled to know with certainty, however, that all relevant electronic data which is resident on the hard drive has been disclosed.[6]

In *Nicolardi v. Daley*,[7] among the issues raised in this solicitor's negligence action was the claim that certain documents were missing from the client's file and that the solicitor had

[6] *Northwest Mettech Corp. v. Metcon Services Ltd.* [1996] B.C.J. 1915 (B.C.S.C., Master Joyce)

[7] *Nicolardi v. Daley* [2002] O.J. No. 595 (Master)

failed to produce all relevant documents. The former client sought an order for inspection of his former solicitor's computer. In considering the request the Master noted that:

> The documents of course must have a semblance of relevance to the issues in the action as framed by the pleadings. When it is alleged by a client that a former solicitor was negligent, or failed to properly prepare for trial or obtain critical evidence, or acted without a client's authority, then virtually every document in the solicitor's file would have a semblance of relevance to the action, if properly pleaded, and would be producible subject to privilege claims. I find that the statement of claim herein is sufficiently particularized so as to require production of all documents in the solicitor's file, particularly as the client has specifically pleaded that the solicitor failed to deliver to him all of the file documents.
>
> Since the definition of document in the Rules includes data stored electronically, then if production for inspection of a document stored on computer is ordered, then such production can only be made if the court orders a hard copy of all documents to be printed, or orders a duplicate of the electronic data be reproduced and delivered on diskette, or allows an inspection of the storage device in which the electronic information resides. Where a party on proper evidence convinces the court that documents have not been produced are likely stored on a computer hard drive or other electronic storage medium, but the party in possession of the computer asserts it has printed and produced all that it has, then the only solution that would allow inspection of a document, would be inspection of the storage medium itself, in this case the firm's hard drive, with proper safeguards.…
>
> It will not be every lawsuit against a lawyer for negligence that will expose the lawyer's computer to inspection by his former client. Actions in which such inspection will be ordered are likely to be rare.…[8]

The court therefore ruled that the electronic evidence was relevant and that the plaintiff was entitled to inspect his former solicitor's computer.[9]

[8] *Nicolardi v. Daley* [2002] O.J. No. 595 (Master) at paras. 28-29, 32

[9] Unfortunately for the plaintiff, the computer was destroyed sometime during the course of the litigation.

In *Dulong v. Consumer Packaging Inc.*,[10] the court held that a broad request from a plaintiff 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".

The burden of producing e-mail was also raised in the case of *Canada v. Air Canada*[11] which dealt with alleged anti-competitive behaviour by Air Canada. Air Canada argued that a section 11 Order under the *Competition Act*[12] would require it to search four years' worth of the 6,000 – 12,000 e-mails received by each of its employees annually and spend two to three weeks recreating the file for e-mail received more than six months prior to the order. While the Federal Court found that the production request made by the Commissioner of Competition was not irrelevant to the inquiry, the court ultimately did not rule on the issue, since the parties agreed to negotiate with respect to the scope of the request.

Courts in the United States have also been responsive to objections to overly broad e-Discovery requests.[13]

Parties should assess the sources of available data and develop a focused discovery request. Overly broad requests may encourage the other side to either bring a motion objecting to the request on the grounds of relevance and inordinate expense, or to drown the opponent in

---

[10] *Dulong v. Consumer Packaging Inc.*, (2000) O.J. 161 (Q.L.) (January 21, 2000, Ontario Master)

[11] *Canada (Commissioner of Competition) v. Air Canada*, [2001] 1 F.C. 219 (T.D.) QL)

[12] *Competition Act*, R.S.C. 1985, c. C-34

[13] See, for example: *INS Corp. v. UPS Fidelity & Guaranty Company*, 122 F.R.D. 567, 570 (N.D.C. al.) 1988, *Sabouri v. Ohio Bureau of Employment Services*, No. CIV. 2.97-715 2000 WL 1620915 (S.D.oh.) October 24, 2000, and *Fennell v. First Step Designs*, 83-F.3D 526, 532 (First CIR. 1996) for cases on the subject of overbroad production requests and undue burden and expense in documentary discovery.

mountains of irrelevant information, which even an expert, may have difficulty sorting through. Extensive production requests may also lead to equally extensive requests for production by opposing counsel.

5. Preserving Metadata

Unlike its paper predecessors, electronic media not only stores the information that is placed upon them, but often carry their own story and history embedded therein.[14] This type of data is called metadata – meaning "data about data". There is a legal presumption in most cases that the producing party need not take special efforts to preserve or produce metadata.

In cases where the requesting party has reason to believe that metadata will be significant, prior notice of this belief should be given to that party. Cases where metadata may be relevant and vital to proving the authenticity of an electronic document includes cases involving allegations of fraud, criminal conduct, espionage, etc. Essentially, any situation where chain of custody issues will be important, will give rise to the need to preserve and produce metadata. However, in reality, most of the metadata has no evidentiary value, and any time and money spent reviewing it is a waste of resources.

6. Costs

Cost is increasingly becoming an issue in e-Discovery cases, because of the huge volumes of material than can be involved and the sometimes staggering cost of processing it. According to the Chicago law firm of Vedder Price Kaufman & Kammholz, restoring e-mail can cost roughly U.S. $2 per message, including the cost of lawyers needed to review the documents.

[14] Matthew M. Neumeier, Brian D. Hansen & Irina Y. Dmitrieva of Jenner & Block, LLC, Chicago, "*Paper or Plastic? – The Hunt for Electronic Treasure during Discovery*", Mealey's Litigation Report: Discovery, Vo. 1. No. 3, December, 2003, at p. 5

A recent article, which appeared in the Chicago Tribune, reported that Exxon Mobil generates 121,000 backup tapes per month, which it routinely recycles according to its records-retention policies. The company claimed that if a judge ordered it to stop recycling tapes to preserve data, the cost just for buying extra tapes would be $1.9 million per month.[15]

Traditionally, the rule has been that each party is responsible for identifying the documents potentially relevant to a suit, giving the other side a list of both documents and allowing access to them. While there is no legal requirement to make copies, the owner of the document usually does this, and the other party pays the cost of copying. In any e-Discovery, the work involved in digging through computer disks in years-old backup tapes has the potential to bankrupt a company and larger organizations bear larger risks and burdens in having to comply with requests.

The simple threat of forcing a corporation to review thousands of files or back-up tapes can, without a doubt, leverage settlement. In recognition of this fact, courts have taken steps to impose additional cost burdens on those parties whose requests for electronic data are determined to be overreaching, spurious or designed simply to force a settlement. On the other hand, where the costs associated with retrieving relevant electronic information are high due to the manner in which the electronic information is stored or the lack of a proper records management policy, the document "owner" or producing party can be required to bear the costs of doing so. The court has discretion to manage and monitor the costs resulting from discovery requests, and to give interim orders concerning costs. Nevertheless, courts seldom exercise this

[15] Ameet Sachdev, "*E-mails become Trial for Courts: Costly Electronic Discovery – Part of Potentially Every Case in the 21st Century*", Chicago Tribune, online edition, April 10, 2005

discretion in a manner which precludes discovery and in exercising the discretion the court does not discount the probity of the allegations.[16]

7. Preservation of Electronic Evidence and Anton Piller Orders

Disputes concerning the admissibility and authenticity of electronic evidence tend to arise more frequently in circumstances where the "chain of custody" is important, such as cases involving fraud or other criminal conduct, where for example, the individual is accused of downloading pornography or hijacking a Web-site. In these circumstances, forensic evidence is most often required to establish or "authenticate" the electronic trail to prove that the impugned conduct took place and to establish the identity of the perpetrator, who often hides behind a pseudonym on the Internet. Other objections to the introduction of electronic evidence may stem from acknowledged or proven security lapses or breaches where unauthorized access to the computer at issue or the computer network is known or becomes apparent. These concerns can be rebutted where proper steps are taken to preserve electronic evidence and where that evidence is produced in electronic form so that the metadata can be accessed and its hidden truths uncovered.

Anton Piller and other types of preservation orders can be obtained to preserve the electronic evidence.[17] By obtaining such an order, the preservation of the evidence is assured and chain of custody issues are more easily defeated.

---

[16] *Sandhu v. Ontario* (1990), 49 C.P.C. (2d) 298

[17] *Computer Security Products Inc. v. Forbes*, [1999] O.J. No. 4573; *Yaghi v. WMS Gaming Inc.* [2003] A.J. No. 1002 (Alb. Q.B.)

In *Canadian Derivatives Clearing Corp. v. EFA Software Services Ltd*., a proceeding brought for breach of a confidentiality agreement and the disclosure of confidential information by the defendant to a third party, the plaintiff sought an Anton Piller order for delivery of the defendant's paper documents and a copy of all of the defendant's electronic data from its computer hard drives in a "mirror image" form to ensure its preservation. The order also enjoined the defendant from misuse of the confidential information. The court upon being satisfied that the Anton Piller/Preservation Order met the test set out in *Anton Piller KG v. Manufacturing Processes Ltd.*, [1976] 1 Ch. 55 (C.A.) noted that:

> Electronic data poses a particular challenge. In a proceeding brought for breach of a confidentiality agreement and the disclosure of confidential information by the defendant to a third party Information about the creation, revision and deletion of data may surface. One of [the plaintiff's] CDCC 's goals is to trace the travels of its Confidential Information through [the defendant's] EFA's system. CDCC suspects that it may be able to find an inappropriate informational link between the CDCC and NexClear [the third party] projects. That endeavour would require certain computer expertise, and may be the subject of a further hearing before this court. For that purpose, preservation of the mirror image copy is essential, Given what is now known about the release of at least some of CDCC's Confidential Information to NexClear and its consultants, this cannot be described as a fishing expedition.[18]

In *Yaghi v. WMS Gaming Inc.* [19] the applicant discovered a method of winning extra credits on certain video lottery terminal games without inserting more money. He informed the manufacturer of the affected machines, WMS Gaming Inc., and demanded payment of $250,000 for information regarding the anomaly. WMS offered $50,000 which was rejected by the applicant, Yaghi, who advised that he would reveal the information publicly unless he received a

[18] *Canadian Derivatives Clearing Corp. v. EFA Software Services Ltd*. [2001] A.J. No 653, at para. 51

[19] *Yaghi v. WMS Gaming Inc.* [2003] A.J. No. 1002 (Alb. Q.B.)

better offer. A few days later there was a posting on a website by a person identifying himself as "zeus_y" indicating that WMS had flaws in its gaming machine software, and that full information would be posted within 48 hours. The web posting contained several defamatory remarks concerning WMS and its "officials". WMS obtained an Anton Piller order requiring Yaghi to permit entry of his premises for search and detention of computer equipment containing relevant information.

8. Preservation Letters and Orders

In cases where parties expect the opposing party to have electronic evidence, it is good practice to send a preservation of evidence letter early on in the process, notifying opposing counsel of the need for steps to be taken to preserve the electronic evidence. If a preservation of evidence letter (or request for a litigation hold) is not sent, opposing counsel may claim that they were not aware that evidence stored on back-up tapes was being deleted (due to the routine rotation of these back-up tapes) or that e-mails were being deleted through an automated process put in place by the organization.

Because of the difficulties inherent in locating and identifying relevant documents, a large organization or business would be unlikely to agree to an order to preserve all electronic records. An overly broad preservation order that attempts to capture everything that may possibly be relevant will undoubtedly and significantly interfere with the operation of that organization or business. A more specific tailored request for preservation is more likely to be considered by the party on the receiving end and enforced by a court.

There are no hard and fast rules dictating how to deal with the issue of preservation. Here is a list of instances where detailed Preservation Notices are appropriate:

- When the substantive allegations involve computer-generated records, i.e., software development, e-commerce, unlawful Internet trafficking, etc.;

- When the authenticity or completeness of computer records is likely to be contested;

- When a substantial amount of disclosure or discovery will involve information or records in electronic form i.e., e-mail, word processing, spreadsheets and databases;

- When one or both parties is an organization that routinely uses computers in its day-to-day business operations during the period relevant to the facts of the case;

- When one or both parties has converted substantial numbers of potentially relevant records to digital form for management or archival purposes;

- When expert witnesses will develop testimony based in large part on computer data and/or modeling or when either party plans to present a substantial amount of evidence in digital form at trial;

- In any potential "big document" case in which cost associated with managing paper discovery could be avoided by encouraging exchange of digital or imaged documents (especially if multiple parties are involved).

This challenge of e-Discovery was addressed in the U.S. case, *Zubulake v. UBS Warburg LLC* ("*Zubulake*"), which is a five-part decision from the United States District Court, Southern District of New York, considering a request for an order compelling UBS to produce at its own expense various e-mails existing only on back-up tapes and other archived media. (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.) According to UBS, restoring such e-mails would cost approximately US $175,000 exclusive of attorney time to review the retrieved data. The *Zubulake* case, involved an action for gender discrimination and illegal retaliation. The court determined that the mere fact that e-Discovery is at issue should not change the rule that the producing party presumptively pays for the production. *Zubulake* stands for the proposition that cost shifting may be considered only when e-Discovery imposes an undue burden or expense on the producing party. The question of undue burden, the court explains, usually turns on whether the electronic information is kept in an accessible or inaccessible format, which in turn depends on the type of media used to store the information. Data stored online or near line, on optical disks, or on magnetic tape media are usually accessible, backup tapes and fragmented data are usually not. Judge Scheindlin ruled that it is not appropriate to consider cost shifting for discovery of active files or date stored on optical disks than can be reach via easily acquired hardware and software.

In *Zubulake Opinion V*,[20] the Court held that counsel's duty to ensure that all relevant information is discovered, retained and produced includes a duty to effectively communicate to clients regarding discovery obligations, identifying sources of discoverable information, speaking to key players in litigation and to the information technology personnel. Where spoliation willfully, intentionally or recklessly occurs and the requesting party shows that the lost discovery of information is relevant to an issue at trial, an adverse inference can be drawn. This decision has been the subject of widespread criticism in the United States for the onerous burden it imposes on counsel to ensure that litigation holds are put in place and followed.

[20] 02 Civ. 1243 (SAS) July 20, 2004

The challenge for counsel is to determine in what circumstances a litigation hold should be put in place. In this regard, the following questions should be answered:

- What steps have counsel taken to ensure that likely discovery material in their clients' possession (or in the possession of third parties) will be preserved until the discovery process is complete?

- If counsel has not yet identified all material that should be disclosed or may be discoverable, what steps have been taken to ensure that material will not be destroyed or changed before counsel's investigations are complete?

Answering these questions is a good place to begin when approaching the dilemmas of preservation of electronic evidence. The remainder of the paper will provide an in depth discussion, including some helpful hints that can aid in addressing the various challenges this developing area of law poses to the legal community.

Part II: Common objections in e-Discovery and Strategies for Overcoming the Challenges of e-Discovery Production

I) Objection on the Ground of Undue Burden and Expense

Objections to requests for electronically stored information arise where the request is deemed to be an undue burden and expense. In determining whether or not a request for production is unduly burdensome, the Court will examine the relative cost and burden to the parties, the need for information, the available sources of that information (to the extent that cheaper and more easily accessible sources are available) and whether the party requesting the information will benefit from the information, in other words, whether or not that party will gain relevant information from the disclosure process. A party raising an objection against overly

burdensome or oppressive requests must educate the Court as to the cost and burdens of the request and argue that the cost and burdens outweigh the value. Be ready to offer reasonable alternatives.

Many cases where objections have been made to overly broad requests for information occur in the context of a request for unrestricted access to a party's hard drive, data or request for on-site access. A request for access to a party's hard drive is akin to requiring production of an organization's entire filing cabinet whether or not the file has anything to do with the case at issue. Other objections are made on the grounds that production and searching for responsive documents on back-tapes, or of deleted files, for example, is unduly burdensome and too costly.

II) Objection on the Ground of Confidentiality Issues

In some cases, issues of confidentiality, such as access to proprietary software to view electronic documents that are otherwise inaccessible, business secrets, or other proprietary information including source code, become contentious where electronic evidence is concerned. While courts are reluctant to restrict disclosure of information to the parties, they will closely examine whether the information being sought is of probative value, particularly where they may not be able to contain the confidentiality of the information sought to be disclosed.[21]. Alan Gahtan's treatise on *Electronic Evidence* sets out the following principles:

- The necessity for complete disclosure in litigation cases supersedes the fact that a party may lose a competitive advantage when disclosure is made.[22]

---

[21] *Deprenyl Research Ltd. v. Canguard Health Technologies Inc.* (1992), 41 C.P.R. (3d) 228 (Fed T.D.); *Devron-Hercules Inc. v. Gill* (1998), 21 C.P.R. (3d) 455 (B.C.C.A.)

[22] *Forestral Automation Ltd. v. R.M.S. Industrial Controls Inc.*, (1977), 4 B.C.L.R. 219; 35 C.P.R. (2d) 114 (B.C.S.C.)

- In maintaining a balance between disclosure and confidentiality, the governing principle is to lean in favour of openness and disclosure.[23]

- The party viewing the confidential materials shall given an undertaking to the court and the opposite party, the terms of which may vary from case to case.[24]

- The party whose documents are being disclosed to be examined by an expert is entitled to have a representative present during the examination.[25]

- An order preventing counsel from showing relevant documents to his client should only be granted in exceptional circumstances.[26]

- The onus is on the party requesting the restriction to establish a legal reason for the restriction.[27]

- In matters that do not require technical expertise, the parties may be required to produce the documents to a third party for the examination and report to the court.[28]

- In instances where the probative value of the documents is not sufficiently great to outweigh the real and considerable adverse effect of disclosing the trade secrets, disclosures ought not to be ordered.[29]

---

[23] *Devron-Hercules Inc. v. Gill* (1988), 21 C.P.R. (3d) 455 (B.C.C.A.)
[24] *GEAC Can Ltd. v. Prologic Computer Corp.* (1989), 24 C.P.R. (3d) 566 (B.C.S.C.)
[25] *GEAC Can Ltd. v. Prologic Computer Corp.* (1989), 24 C.P.R. (3d) 566 (B.C.S.C.)
[26] *Deprenyl Research Ltd. v. Canguard Health Technologies Inc.* (1992), 41 C.P.R. (3d) 228 (Fed. T.D.)
[27] *Deprenyl Research Ltd. v. Canguard Health Technologies Inc.* (1992), 41 C.P.R. (3d) 228 (Fed. T.D.)
[28] *Webster v. Mastercraft Development Corporation* (1991), 55 B.C.L.R. (2d) 121 (B.C.C.A.) [In Chambers]
[29] *G.W.L. Properties Ltd. v. W.R. Grace & Co of Canada* (1992), 70 B.C.L.R. (2d) 180 (B.C.S.C.)

Strategies for Overcoming Challenges of e-Discovery Production

1. Know Your Case and Your Client:

It is important to understand the organizational structure of the opposing party and the type of documentation generated by the business. Speak to employees within your own client's information technology (IT) department who will often be of great assistance in not only explaining the client's computer systems, records generation and retention practices, but will also be able to provide useful insight into your opponent's IT systems as well.[30]

2. The Client's Electronic Information

To best preserve relevant information and locate it, at the outset, learn and understand the following about your client's computer system:

(a) Operating systems and applications programs;

(b) The location of computer data files both active and archived (this may include computer files on an employee's computer or other device, whether at home or at the office;

(c) Determine what databases, e-mail, word processing documents and other computer data are relevant to the dispute;

(d) Determine the cost of locating, reviewing and producing relevant information (this would include the cost to convert or extract data from legacy systems into a useable format for analysis and production);

(e) Determine the structure of the e-mail system. (Since e-mail is one of the most sought-after forms of electronic information, one must have a clear understanding of a client's e-mail system. This should include present and prior e-mail systems that the client used, such as Lotus Notes, Microsoft Outlook, etc.);

(f) Determine what document and other computer data file retention policies are in place, and whether there is an immediate necessity of stopping the deleting or purging of data files that may be relevant to the case;

[30] Michael R. Arkfeld, "*Electronic Discovery and Evidence"* (Phoenix: Law Partner Publishing, 2003) at 3-7.

(g) Determine accessibility issues for each computer location, device or media such as passwords, security and encryption keys;

(h) Consider segregating responsive electronic data on a dedicated computer for storage and review;

(i) Determine the necessary of retaining a forensic specialist to assist in the discovery and/or disclosure of computer data;

(j) Avoid spoliation charges by ceasing the automatic recycling of back-up tapes and installation of new hardware once you are put on notice that a claim is going to be asserted; and

(k) Determine the capability of your client to search and retrieve data requested by the opposing party.

3. Solutions to Defining Requests

Narrow your e-Discovery request by:

(a) Identifying the "persons of interest" and their work groups (consisting of secretaries, administrative assistants, supervisors, etc.), who work closely with those intimately involved in the matters at issue.[31]

(b) Make a specific request for the preservation of data (if required) and the provision of information on storage devices (network drives, local hard drives, floppy disks, removable drives, portable computers, home computers, etc.)[32] used by the persons of interest and their work groups.

(c) Assess the relevance of searching the files of persons who are peripherally involved or who were simply copied or kept informed.

4. What to Ask For to Help Limit the Volume to Relevant Documents

It is important to note that the nature of the case will help to define the type and source of electronic information sought. For example:

(a) A case on Internet Usage will focus on internet logs, usage patterns, browser history, downloaded Internet files, etc.

(b) A wrongful dismissal case or case involving misuse or theft of confidential information by a former employee may concern the "unlawful use" by that employee

[31] Gregory S. Johnson, "*A Practitioner's Overview of Digital Discovery*" (1997) 33 Gonz. L. Rev. 347 at 364
[32] Gregory S. Johnson, "*A Practitioner's Overview of Digital Discovery*" (1997) 33 Gonz. L. Rev. 347 at 364

of the internet to "transfer" corporate information via email to their new employer. Similarly, a wrongful dismissal case may involve employees engaged in other illicit activities such as viewing of pornography from corporate computers. This type of case will also focus on downloaded internet files, internet logs, firewalls, e-mail, cookies, websites stored on favourite folders, and would mostly likely require hard drives to mirror-imaged or "ghosted" to "preserve" the evidence.

(c) In cases involving allegations of fraud, theft of confidential information or where "chain of custody" regarding computer usage or abuse of computer usage is relevant, it is important to take steps to preserve that chain of custody. It is in these kinds of cases that metadata is most likely to be relevant and producible. Therefore, unless the producing party is aware or should be reasonable aware that particular metadata is relevant; the producing party should have the option of producing all, some or none of the metadata.

(d) A case involving a business dispute concerning anti-competitive matters would be more likely to focus on electronic messaging, customer databases, memos and letters, sales figures and marketing messages.

Once you know what and where to look for documents, e-Discovery can further be streamlined to help narrow the scope of production, reduce the quantity of documents and cost of the process by implementing several of the following limiting tactics.

5. Filtering

Filtering electronic information is reducing the size of the electronic file population by limiting computer files to specific search criteria, such as keywords, names, specified dates, etc. The necessity of engaging in this process is due, in large part, to the way in which computer fields are stored. As explained earlier, electronic files are not organized in the same manner as paper files. E-mails, for example, are often disorganized with the e-mails for any one individual on any particular day covering a wide range of topics, customers and issues. Through the use of filtering software, those e-mails relevant to the case at hand are identified. It also protects an organization from producing otherwise confidential or sensitive material that a company might be loath to disclose to a "competitor".

As an example, the following data search protocols should be considered:

(a) Date/time range limits. One search parameter would be to limit the date or time range for e-mail, word processing documents or other electronic information.

(b) Author, recipient or other key personnel. Consider limited searches to individuals by name, title or other references relating to the subject matter of the litigation. Key search terms would include e-mail addresses of certain individuals or names of individuals in the subject line.

(c) Key terms -- a list of the key terms can be developed that are common to the claim and/or defences set out in the pleadings.

(d) Certain data file types. One can search by data file types in order to limit the electronic data population.

These search techniques can be used to further reduce the amount of electronic information that is identified as being potentially relevant and that therefore must be reviewed. Such techniques therefore help to reduce the time and cost involved in the collection, retrieval and review of electronic information.[33]

6. De-Duplication

De-duplication or "de-duping" means a process of separating duplicate e-mail or electronic messages, word processing documents or other computer files from "duplicate" electronic files. For example, people often send the same e-mail messages to more than one recipient or word processing document to multiple recipients. Most software companies involved in the collection and management of a database containing the potentially relevant documents will attempt to de-dupe the documents. However, a technical de-duping identifies only those documents with the same "hash" values.[34] Therefore, what looks like a duplicate to

[33] Michael R. Arkfeld, "Electronic Discovery and Evidence", at page 6.26

[34] A **hash function** or **hash algorithm** is a function for summarizing or probabilistically identifying data. Such a summary is known as a **hash value** or simply a **hash**, and the process of computing such a value is known as **hashing**. A fundamental property of all hash functions is that if two hashes (according to the same function) are different, then the two inputs were different in some way. This property is a consequence of hash functions being

the human eye will not always be identified as a duplicate by a computer. The de-duping process can be determined by the parties and can include matches for the author, recipient, subject line, date, time of creation of the e-mail and other criteria. You should be aware that to "de-duplicate" does not necessary mean destroying or deleting duplicates from the electronic file information. Generally speaking, it means that documents are labeled as duplicates and then tied to the original message or word processing document.

7. Backup Tapes

The need for discovery of backup tapes should always be demonstrated by supportable evidence, including evidence that responsive documents are likely to exist, and have otherwise been destroyed or lost. There are many technical and practical obstacles to the search of backup tapes. The purpose of backup tapes is to protect against the loss of information caused by computer failure. Often, special consultants or experts must be retained to restore the backup tapes to a searchable form and to enable the search and retrieval of identified files. The disbursements or expense of the search, conversion and retrieval of electronic data on backup tapes can be very costly so it is important to recognize when it is necessary to take this route.

8. Sampling of Computer Data

One possible response to an undue burden argument being advanced by an opposing party, as well as a solution to combat the problems of volume and defining your request, is to do a "sampling" of computer data. Sampling involves conducting test runs of data to statistically

---

deterministic, mathematical functions, but they are generally only surjective functions (i.e. not necessarily one-to-one). Consequently, the equality of two hash values does not guarantee the two inputs were the same, but in some cases, probability theoretic or computability theoretic guarantees apply.

determine the volume of relevant data available in the computer files. In *McPeek v. Ashcroft.*[35] the court required the Defendant, the Department of Justice, to restore, at its own expensive, e-mail "attributable to [one supervisor's] computer" as a "test run" to decide how to approach further discovery of any computer evidence of retaliation. In the *Zubulake* case, the court also successfully implemented a sampling in order to better weigh the veracity of extensive e-Discovery request.[36] Sampling is a cost effective mechanism, which when implemented in association with a well worded, date and key player specific request, can greatly assist a Court to decide or assist parties to negotiate the value and breadth of scope for an e-Discovery request.

9. Retaining an Expert

Due to the highly technical nature of electronic data, it may be prudent to hire an outside expert or forensics technologist to both draft a plan of review and conduct the actual examination of the recovered material. Even on a basic Internet search, forensic experts can find relevant evidence about your opponent by tracking their Internet searches. In *People v. Smith,*[37] a decision rendered in California, the defendant's Internet searches, located by the expert, showed that he was tracking down the victim.

There are many advantages to retaining an expert, including the following:

(a) An expert knows there to look for the information required, and can help tailor discovery requests if you need to narrow discovery while procuring as much useful information as possible.

(b) An expert can duplicate the media for analysis without altering the original. An investigation of electronic data should never be undertaken on original media since such key system information as the date the last file was open or revised could be changed.

---

[35] *McPeek v. Ashcroft* 202 F.R.D. 31, 34 (D.D.C. 2001)
[36] *Supra* note 14.
[37] *People v. Smith* 2001 WL 1264553 (Cal. App. 6 Distr. October 23, 2001)

(c) An expert can recreate the native environment required to restore data and analyze evidence.

(d) An expert can recover data from obsolete systems, unearth data that has been "deleted" from the media, and provide evidence of tempering or selective disclosure.

(e) An expert can not only find the data, but can also obtain information about the data, such as when it was created, who accessed it and when, and all copies which were made.

(f) An expert can help preserve the chain of custody and prove authenticity of the evidence. An expert is far better qualified than an attorney or an IT staffer to explain the technical side of computer forensics and defend against common charges that the evidence is unreliable or that it was subject to tampering.

Conclusion

In principle, e-Discovery is the same as any other type of document discovery. However, as is evident from the above discussion, the practice of actually retrieving electronically stored information also makes e-Discovery unique from other types of discovery. The actual physical location of an electronically stored document varies on a spectrum between accessible and easily produced to inaccessible and difficult to produce. Many factors have to be considered when requesting or responding to an e-Discovery request. These factors include: recognizing the potential volume of documents, considering the use of key search terms to help to identify relevant documents, deciding what type of information is actually needed, locating the key players, and taking steps to ensure that electronic evidence is not lost through ordinary useage. The benefits of electronically stored data should not be overlooked and lawyers who do so risk leaving potentially critical information undiscovered.

Just as the use of computers has increased efficiency in communications with clients and productivity in our respective practices, there is a vast potential for the benefits of technology to assist in making documentary discovery more fruitful. We encourage you to consult the e-

Discovery Guidelines which were prepared to provide guidance to members of the Ontario Bar in dealing with e-Discovery issues.

Authored By:	Karen Groulx Pallett Valo LLP	Sara Blake Ministry of the Attorney General
Assisted By:	Michael Nowina Pallett Valo LLP	Julia Candeloro - Articling Student Pallett Valo LLP

Q:\Litigat\Karen\Making and Responding to Requests for Electronic Discovery- Final