PAPER:

SEARCH AND SEIZURE OF DIGITAL EVIDENCE: THRESHOLDS AND MINEFIELDS

By **Justice J. E. (Ted) Scanlan,**
Justice of the Supreme Court of Nova Scotia and Deputy Judge of the Nunavut Court of Justice

Discovery and document production is a common part of litigation world wide. By some estimates, more than ninety percent of all information is now created in electronic format.

The explosive growth and diversification of electronic documents and communications has transformed the meaning of the term document. In most, if not all, jurisdictions electronically stored information is discoverable. As a general rule relevancy is the pre-requisite to production, regardless whether the medium is paper or electronically stored information. I use the term electronically stored information as opposed to electronically stored documents because there are many possible types of electronically stored information that may not necessarily constitute what we would think of as being equivalent to a normal paper document. The term electronically stored information is meant to be all encompassing.

The many unique characteristics of electronically stored information have created challenges and burdens for litigators, litigants and the courts. These characteristics include the fact there are large volumes of electronically stored information. That information is created at rates that are much greater than paper documents. Electronically stored information is hard to dispose of. In spite of any attempt to delete electronically stored information, it may remain in an electronic storage device. The persistence of electronically stored information compounds the rate at which it accumulates in places hidden from the user. A user may have no idea that the information is still on the computers. Electronic documents often include meta data which creates unique issues for production of documents in litigation. Electronic documents are often updated in systems without the user even being aware of the changes taking place. In those situations it may be difficult for the user to decide which version of the data base is appropriate for production in discovery or what is called the disclosure process in England and Wales.

There is also the need for a computer program to interpret electronically stored information into a comprehensible form. Unlike paper data where the information is static, with electronically stored information, systems are often replaced or become obsolete. The question then becomes how to make sense of data which is stored and no longer has a system which is able to read and interpret the data. This creates unique issues for recovering 'legacy data'.

In most organizations electronically stored information may be stored in many locations or on many devices. Think for example about the number of computers that may be linked to a server, and ask who may have downloaded information. What of the CDs and backup tapes, hand held digital devices, even photocopier and facsimile machine digital memories, laptop computers, digital voice recorders, chat lines, and such like. The wide range of possible locations for information makes certification as to production almost impossible. This has come to the forefront in the United States of America where courts have been making huge punitive awards in cases where law firms have certified complete production and it transpires that some documents have not been produced. The awards are against both clients and law firms and are in some cases several hundreds of millions of dollars.

I dare anybody in any large or medium sized corporation or government to try to explain the full network system and certify that they have produced all information relevant to a matter. It is impossible for even those with the most comprehensive understanding

of those systems to certify that all of the electronically stored information has been retrieved from all possible locations within any organization. Think for example of an e-mail that may have been at one time stored on a corporate or government system that has since been fully deleted. A copy of that e-mail may have been forwarded to a Blackberry by an employee, and it could be stored on the hand held device. These unique difficulties in dealing with electronically stored information are more fully discussed in the Sedona Canada Principles published January, 2008.[1]

The topic of my paper is 'Search and Seizure of Digital Evidence: Thresholds and Minefields'. The thresholds in terms of obtaining access to information is relatively low. As mentioned earlier, if information is material and relevant, in most jurisdictions it can be obtained. In emergency situations, which will be discussed in greater detail, there is the additional requirement to show that information will be lost or destroyed if a preservation or seizure order is not granted. A wide review of Civil Procedure Rules makes it obvious that electronically stored information is producible and generally the courts will order production of electronically stored information providing it is not privileged or protected from production. Many jurisdictions do not allow a party to withhold electronically stored information which is relevant and material in situations other than where privilege or specific protections are afforded. There are exceptions to this.[2]

There are some differences in various jurisdictions. For example, in Canada there is generally a positive duty on each party in the litigation to produce potentially relevant documents. In the United States a production obligation stems from an obligation to respond to specific production requests. If a document is not requested it need not be produced even if it is relevant. In the 'Civil Law' Jurisdiction in Canada (Quebec) there is an entirely separate regime in which there is no general duty to produce potentially relevant documents and indeed there is not even a duty to preserve potentially relevant documents unless the court specifically orders the preservation or production. Having said this, electronically stored information is routinely produced in Quebec without a specific obligation to do so.

The situation in England and Wales, as I understand it, requires a litigant, pursuant to Civil Procedure Rule, Part 31, to conduct a reasonable search for relevant documents. There is a duty to give standard disclosure of any documentation upon which a party may rely as well as any documentation that may adversely affect one's case or adversely effect or support another person's case.

It has been long established in England and Wales that a document includes a computer data base.[3]

In many jurisdictions the Civil Procedure Rules have established specific guidelines for litigants in dealing with access to electronically stored information. In most jurisdictions there is an increased role for the judiciary in the management of, the extent and expense of recovery of electronically stored information. It places a duty on judges to conduct active case management in order to deal with matters expeditiously, fairly and proportionately. Most jurisdictions have adopted or are in the process of adopting guidelines to assist the courts and parties in determining what a reasonable search is. Civil Procedure Rule 31.7 in England and Wales lists a number of factors to help judges determine what constitutes a reasonable search. They include:

a. the number of document involved;
b. the nature and complexity of the proceedings;
c. the expense in retrieving any particular document; and,
d. the significance of any document which is likely to be located during the search.

To one degree or another these appear to be universally considered factors. Courts should be particularly cognizant of issue of expense in relation to retrieval in general, and more specifically the cost of identifying and separation of privileged documents. There have been a number of situations in Canada and elsewhere where litigants have requested orders requiring parties to disclose electronically stored information without realizing the scope and nature of the search required to fulfill or comply with the order. What may look like a simple order, which could be easily complied with, may in fact place a burden on a party requiring an expenditure of many millions of dollars in search and retrieval of electronically stored information. I would argue that because of the unique characteristics of electronically stored information, there has to be a new approach to production or the entire justice system is in danger of collapse. Few parties could afford to litigate on the merits if we do not take a different approach.

[1] *http://www.lexum.umontreal.ca/e-discovery/Sedona Canada Principles 01-08.*
[2] *See Stephen Mason, general editor, International Electronic Evidence, (British Institute of International and Comparative Law, 2008).*
[3] *See Grant v South Western and County Properties Limited [1975] Ch. 185 or Derby & Co. Ltd. v Weldon (No. 9) [1991] 1 W.L.R. 652.*

Searching and disclosure should be subject to a test of proportionality. In some jurisdictions courts will impose the requirement to do key words searches or other forms of searching as agreed upon between the parties. Under the Sedona Canada Principles, the parties would be required to meet and confer early and often in an attempt to agree to things such as search terms and parameters, locations of searches, data bases, and such like. If the parties are not able to agree on these issues, then the court would become involved and set those parameters or search terms. New Civil Procedure Rules soon to be implemented in Nova Scotia actually incorporate the Sedona Canada Principles by reference in the Rules.

In the United Kingdom, there are relatively few reported cases with regard to the balancing of factors and interests at stake. There is a recent case *Dome Telecom v Eircom*,[4] from the High Court of Ireland where the court held that a defendant could be ordered to produce a special report from a data base. The defendant raised concerns about proportionality. In the circumstances of the case, a separate majority held there were significant costs and burdens involved in the preparation and production and that it would be disproportionate to the benefits that such a report would provide, unless the defendant was proved liable. Only then would the plaintiff be entitled to file a new application for discovery if he succeeded in proving the defendant guilty. With regard to the matter of requiring a party to 'create documents' Mr Justice Geoghegan commented, at page 29, to the effect that the form of the data storage may not be relevant to how such data is produced. Geoghegan, J also said:

> In order to achieve a reasonable parity with traditional documentary discovery it may well be necessary to direct a party *"to create documents"* within the meaning of the notice of appeal. ... even if such *"documents" "do not exist at the time the order is made"*.

At page 30 Geoghegan, J noted that:

> But discovery may be "necessary" and yet so disproportionate as to render it unreasonable for a court to benefit the party seeking such discovery by making the order.

Courts in Canada and the United States appear to be willing to require production more willingly, even if it is disproportionate, if there is an agreement by the requesting party to a shifting of costs.

I also refer to *Mulcahy v Avoca Capital Holdings Ltd*.[5] This is a case from the High Court of Ireland. Mr Justice Clarke reasoned that the plaintiff was not necessarily entitled to any of the information on certain computers due to the potential that private materials might be present that were not relevant. In Canada, the approach is somewhat different. Access is usually granted subject to rules prohibiting disclosure of any irrelevant and private information. There are exceptions, however, where the database may include information that would be damaging in terms of trade secrets or sensitive commercial information. In such situations, special steps can be taken similar to the use of a supervising solicitor to ensure that collateral damage does not occur as the result of a competitor obtaining sensitive information.

The whole issue of privilege has created a nightmare scenario for courts, litigants and litigators, when dealing with electronically stored information. In *Mulcahy*, Mr Justice Clarke noted that the litigant:

> Does not have a legal entitlement to look at any more than is necessary.

Part 31.16 of the Civil Procedure Rules in England and Wales introduced the concept of 'pre-action disclosure' as a means of ensuring the preservation of data and of ultimately reducing costs and delay in a proceeding. If an application is made to the court for disclosure before proceedings begin, the court may make an order specifying the documents or class of documents that the respondent must disclose, and may require the respondent to specify any documents which are no longer in his control or over which he claims a privilege or a duty to withhold.

Civil Procedure Rule 31.3 provides that a party to whom documentation has been disclosed is entitled to inspect the document(s), subject to three exceptions, and I refer specifically to exception number two, 'the document is privileged in some manner'. In *Derby*, Vinelott J, identified a variety of difficulties that should be addressed in the course of applying for inspection and copying of electronic documents, and prior to allowing electronic disclosure. He noted that there must be a means to screen out irrelevant or privileged material before an inspecting party can obtain access to the computer. In addition, Civil Procedure Rule 31.20 protects against misuse of inadvertent inspection of

[4] *[2007] IESC 59.*
[5] *[2005] IEHC 136.*

The court said in that case that the fact opposing counsel had potential access to privileged materials overrode the right to counsel, and the firm was removed from the file.

privileged documents which could easily arise during electronic discovery. In that Rule, a privileged document that was inspected may only be used with the permission of the court. In Canada and other jurisdictions, there does not appear to be a similar provision in the Civil Procedure Rules. Common law would suggest that privileged documents that are inadvertently disclosed to the other party should be returned and that privilege is not waived. This is an entirely separate issue upon which an entire paper could be delivered. For the purposes of this paper, I simply suggest that great care should be taken so as to ensure that privileged documents are not released as a result of disclosure of electronically stored information. In Canada, a common law consideration on the issue of waiver of privilege is whether sufficient care was taken to ensure that privileged documents were not disclosed. The issue of privilege arose in a unique way in a case that I was involved in, *National Bank Financial Ltd. v Daniel Potter et al*.[6] There are a number of reported decisions in that case dealing with the issue of privilege. I simply summarize by noting the corporate owner of the electronically stored information hired a company to make digital images of the corporate servers. Eventually the company hired to perform that storage task had a falling out with the principal. There was also continuing litigation between the principal and a lender. The person hired to do the imaging, unbeknownst to the corporation, turned the information over to the solicitors for the lenders. Those solicitors then started browsing through the information at will, including a review of solicitor-client communications. Eventually I ruled that the solicitors should not have been reviewing the information and the corporation had not waived privilege through its actions. The result was that the solicitors for the lenders were removed from the file and there was a substantial order for costs made against the lenders. The lender had to pay costs to a number of other litigants who had been joined in the action and who were either included or joined willingly in the litigation.

In urgent situations there are a number of different means by which electronic information can be obtained or recovered with the assistance of the court. In Canada we use the 'Anton Piller Order'. An Anton Piller Order allows a private citizen to apply, on an ex parte basis, for an emergency order entitling them to enter upon a premises to retrieve or secure documents, including electronically stored information. One of the most difficult issues when acting pursuant to an Anton Piller Order is to prevent contamination of the parties as a result of obtaining access to privileged information. An Anton Piller Order, is the most drastic civil remedy available, but it does not allow a party the right to inspect privileged documents.

Courts in every jurisdiction must be aware of the issue of privilege, and steps must be taken to guard against inadvertent disclosure or access to the privileged information. This was at the forefront in *Celanese Canada Inc. v Murray Demolition Corp*.[7] This case involved allegations of industrial espionage. An Anton Piller order was granted but it did not contain a provision dealing with privileged documents. About 1,400 documents were thought relevant and downloaded and sealed but not screened for privilege. Also, a complete list of documents was not made in accordance with the requirements of the Anton Piller order. Finally, an accounting firm opened the sealed documents, potentially tainting the executing law firm. The court said in that case that the fact opposing counsel had potential access to privileged materials overrode the right to counsel, and the firm was removed from the file. The court noted that an Anton Piller order authorizes a private party to enter the premises of its opponent to seize and preserve evidence to further its claim in a private dispute. The only justification for such an extraordinary remedy is that the plaintiff has a strong *prima facie* case and can demonstrate that absent such an order there is a real possibility that relevant evidence will be destroyed or otherwise made to disappear. There must be threefold protection included in the process or the order: first, carefully drawn order which identifies

[6] *2004 NSSC 100.*
[7] *2006 SCC 36.*

the material to be seized and sets out safeguards to deal, amongst other things, privileged documents; second, vigilant court-appointed supervising solicitor, independent of the parties; and third, a sense of self-restraint on the part of those executing the order with a focus on the limited purpose of the order, namely preservation, not exploitation.

Similar provisions are included in Practice directions giving High Court Judges power to grant 'search orders' and 'freezing injunctions'. I will not go through the provisions of the Practice Direction CPR Part 25, but point out that the court has the power to authorize search and seizure on an inter parte or ex parte emergency basis. The rule even allows a telephone application in cases of extreme urgency. Like Canadian Anton Piller Orders, we see the requirement to have a 'Supervising Solicitor' who has a duty to explain among other things, the terms of the order and the right to obtain counsel. The rule also limits the materials that can be removed to materials that are clearly covered by the order. The rule provides for access to computers, even requiring the respondent to give passwords to enable the search of computers. If the password is not handed over there are remedies. In Canada, we would likely contact the justice who issued the order in the first place and amend the order to enable the computer to be removed until the password could be bypassed by the IT staff in the presence of the Supervising Solicitor. There are also other possible remedies in terms of punitive orders that may allow for the striking of claims or defences in those types of cases.

These types of access orders are generally available in most jurisdictions in one form or another. I expect the same protections are not afforded universally in terms of use of supervising solicitors and protection of privilege.

In the global economy, we must also be aware that what we do in one jurisdiction may have an effect on litigation in other jurisdictions. In *Wilson v Servier Canada Inc.*,[8] Canadian courts considered a US court order which stated that the production of documents were for US litigation only and the documents were not to be used in any other jurisdiction. The case considered products liability dealing with weight loss medication that was allegedly related to some deaths. It was sold internationally. The matter came before the Canadian courts, and the Canadian courts ordered the defendant to produce the documents in the Canadian litigation, overruling the US court imposed limited purpose order.

Courts should also be cognizant of the different rules in different jurisdictions. In *Hopson v Mayor of Baltimore*[9] a US court noted, for example, that 'clawback' agreements, while upheld in some jurisdictions, may not be enforced or respected in other jurisdictions. A clawback agreement allows the release of information without screening on the understanding that if privileged documents are included, they will be returned and the initial release does not amount to a waiver of privilege. Even if that were respected in the jurisdiction where it occurred, it may not be in another. A client would not be happy to find they lost privilege in another jurisdiction. I make this point only to highlight the need to be vigilant in the execution of search orders, because while in one jurisdiction there may be a way to resolve an error, it may not be respected in another jurisdiction.

In summary, the threshold in obtaining electronically stored information is not all that different than it was for paper documents. There is, however, an increasing recognition that the production of the information may be a substantial operational burden and expense. In addition, the volume of material may make the separation of privileged information difficult. The production orders may have ramification in litigation in other jurisdictions. If courts are to remain as a tool for litigants to resolve their differences ,we are going to have to find more affordable ways to allow parties to obtain access to relevant information and to get it before the courts.

Justice Scanlan helped to found, and is a member of the editorial board of Sedona Canada, which develops guidelines to deal with electronically stored information in litigation. He is also a frequent presenter with the National Judicial Institute of Canada and co-chairs the International Faculty Development program to train Canadian judges.

[8] *2002 CanLII 3615 (ON.S.C.).*
[9] *232 F.R.D. 228 (D. Md. 2005).*

