dentons.com

DENTONS

ADMISSIBILITY: UNDERSTANDING TYPES AND SOURCES OF ELECTRONIC EVIDENCE

By: Karen Groulx and Chuck Rothman
With help from Maria Zawidzki

January 19, 2011

Contact

Karen Groulx
Dentons Canada LLP
Partner

karen.groulx@dentons.com
D +1 416 863 4697

Chuck Rothman
Wortzman Nickle Professional Coroporation

crothman@wortzmannickle.com
D +1 416 642 9018

The Power of the "Written Word" and Importance of Electronic Evidence

The primary tool-of-the-trade for litigation counsel remains information: who did what, to whom, and when. As every good trial counsel knows, nothing is more powerful than a document that speaks for itself that cannot be challenged in the usual ways, such as by cross-examination. The advent of the computer age and in particular, the increased use of electronic communication in business, has created a proliferation of potentially available tangible evidence for use in future litigation.

Specific Types of Electronic Evidence

E-Mails

E-mail is currently the most commonly used service on internal networks and the most sought after form of electronic evidence in most cases. E-mail messages are often not reviewed by the organization and typically reflect the personal opinions of the parties of the communication. Nevertheless, courts and regulatory authorities may construe these "off the cuff' comments to reflect the views of both the organization and the sender.

As stated by one legal commentator, "E-Mail is a truth serum".1 E-mail messages have played a prominent role in several recent high profile cases and, as set out previously, are useful as they generally provide access to informal comments that would not otherwise be committed to writing.

Commentators have noted that e-mail undermined the credibility of Microsoft's witnesses and provided the basis for the anti-trust ruling. As set out in Michael R. Arkfeld's treatise on "*Electronic Discovery and Evidence*", citing from Ken Aruletta's publication entitled "*World War 3.0 Microsoft and Its Enemies*":

> Though Microsoft argued that the government's case "relie[d] heavily on snippets of Microsoft e-mail messages that are taken out of context," id. at 67, these e-mails provided support for the District Court's liability findings, upheld on appeal, because "[e]ven in context, to read many of Microsoft's internal e-mails is to be struck by their arrogance." *Id*. at 73. These e-mails became important ingredients in spicing up the government's proofs of anticompetitive behaviour, intent, and lack of credibility of Microsoft's witnesses.2

The New Media

As new media, such as social networking websites like Facebook and MySpace, Twitter, LinkedIn and blogs, increasingly changes the way the world communicates and interacts, it is not surprising that, much like e-mail messages, postings, tweets, pictures and profiles make their way into evidence in many cases. Facebook's Factsheet brags that the social networking site has over 500 million active users worldwide.'

---

1 Bannabum D., "Daemon Seed- Old Email Never Dies", Wired, 7.05 (May) 1999, 100-11

2 Ken Auletta, "World War 3.0: Microsoft and Its Enemies", 55, 489 (2001) as cited in M.R. Arkfeld, Electronic Discovery and Evidence, loose-leaf (Phoenix, Ariz.: Law Partner Publishing, 2003), at 1-17

Facebook, "Facebook Statistics", online: Facebook <http://www.facebook.com/press/info.php?statistics> (last visited Oct. 7, 2010).

As of October 4th, 2010, Twitter reports 165 million registered users4 and LinkedIn claims over 80 million members in over 200 countries.5 While MySpace used to be the leader among the social networking sites, its numbers have seriously declined, with estimates of 122 million users around the globe.6 In fact, the use of social networking sites is so widespread that some experts in the industry have predicted that social media will replace e-mail as the primary vehicle for interpersonal communications for 20 percent of business users by 2014.7

Such electronic data can often serve to disprove claims and defeat cases as it contains uncensored personal information the parties assumed were off limits due to their seemingly private nature. To the contrary, however, the courts have taken the view that where the evidence contained in such sources of electronic data is relevant to the matters at issue in the action, preservation and production of the evidence should be ordered subject to principles of proportionality' imposed by *Ontario's Rules of Civil Procedure*9 .10 As a result, in many recent Canadian decisions, photographs of parties that had been posted to their Facebook profiles were admitted as relevant documents subject to production.11

To illustrate the point that few areas of our daily lives are immune from the effects of new media, consider the story of a Quebec woman who lost her insurance benefits because of the photos posted on a popular social networking site. The woman was on long-term sick benefits for a year and a half after she was diagnosed with major depression. Her insurance company, Manulife, cut off her benefits after seeing photos posted on Facebook of the woman having a good time at a Chippendales bar show, at her birthday party and on holiday.

---

4 Twitter, "#newtwitterceo" Twitter Blog (4 October 2010), online: Twitter <http://blog.twitter.com/> (last visited Oct. 7, 2010).

5 Linked In, "About Us", online: Linked In <http://press.linkedin.com/about> (last visited Oct. 7, 2010).

6 MySpace, "Fact Sheet", online: MySpace Press Room

<http://www.myspace.com/pressroom?ur1=/fact+sheet> (last visited Oct. 7, 2010).

Joel Patrick Schroeder, "United States: Social Media in Civil Litigation" (October 15, 2010), online: Mondaq http ://www.mondaq. com/unitedstatesiarticle. asp?articleid= 112916.

8 See Rule 29.2 of Ontario's Rules of Civil Procedure, R.R.O. 1990, Reg. 194. See also The Sedona Canada Conference Commentary on Proportionality in Electronic Disclosure & Discovery: A Project of The Sedona Conference Working Group 7 (WG7) Sedona Canada, (The Sedona Conference: October 2010). [Sedona Commentary]

9 R.R.O. 1990, Reg. 194 [Rules of Civil Procedure].

1° See Kent v. Laverdiere (2009), 78 C.P.C. (6th) 182, 2009 CarswellOnt 1986 (Ont. Master) [Kent] at ¶ 31 where Master Haberman refused to order the production of three Facebook and MySpace profiles, reasoning that before the preservation and production will be ordered, "there must be something to suggest at least some possible connection between the matters in issue and the documents sought."

11 Ibid., Kent at ¶ 23: Photographs of parties posted to their Facebook profiles have been admitted as evidence relevant to demonstrating a party's ability to engage in sports and other recreational activities where the plaintiff has put his enjoyment of life or ability to work in issue: Cikojevic v. Timm, 2008 BCSC 74 (B.C. Master), para. 47; R. (C.M.) v. R. (0.D.), 2008 NBQB 253 (N.B. Q.B.), paras. 54 and 61; Kourtesis v. Joris, [2007] O.J. No. 2677 (Ont. S.C.J.), paras. 72 to 75; Goodridge (Litigation Guardian of v. King (2007), 161 A.C.W. S. (3d) 984 (Ont. S.C.J.) [2007 CarswellOnt 7637 (Ont. S.C.J.)], para. 128. In one case the discovery of photographs of a party posted on a MySpace webpage formed the basis for a request to produce additional photographs not posted on the site: Weber v. Dyck, [2007] O.J. No. 2384 (Ont. Master).

Manulife took the photos as evidence that she was no longer depressed and told her that she was available to work because of the information gleaned from Facebook.12

Content posted on social networking websites such as Facebook has not only gotten the parties to litigation in trouble, but their counsel too. For example, when a lawyer in Texas asked Judge Susan Criss for a continuance because of the death of her father, the continuance was denied because her story in court did not match her Facebook posts - a string of status updates detailing her week of drinking, going out and partying.13

With respect to a party's preservation and production obligations, it has been held that if there is evidence that material posted on one's Facebook site is relevant to an issue in an action, whether the user's account is strictly public, private or a hybrid of the two, the information is producible.14 Therefore, it is very clear that counsel needs to be aware of the cases relating to the preservation and production of documents contained on Facebook, and in new media such as MySpace, Twitter, etc.

In many recent Canadian decisions, photographs of parties that had been posted to their Facebook profiles were admitted as relevant documents subject to production.15 For example, in *Murphy v. Perger*16, Madam Justice Rady considered the relevance of information contained on the plaintiff's Facebook site to her claim. The plaintiff claimed damages for personal injuries that she alleged were sustained **in a motor vehicle** accident with the defendant. The plaintiff advanced a claim for general damages for pain and suffering and loss of enjoyment of life. A central issue quickly became the production of photographs displayed on the plaintiff's private section of her Facebook account.

Madam Justice Rady allowed access to the private Facebook site in light of a number of factors. The Court had to be satisfied that the document was relevant to an issue in the proceeding.17

---

12 "Depressed woman loses benefits over Facebook photos" CBC News (21 November 2009), online: CBC News <http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html> (last visited October 8, 2010).

13 Molly McDonough, Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches, ABAJournal ¶ 5 (Jul. 31, 2009),

http://www. abajournal. com/news/facebookingjudge_catches_lawyers_in_lies_crossing_ethicaliines_aba chicago.

14 Leduc v. Roman, 2009 CarswellOnt 843 at ¶ 15.

15 Frangione v. Vandongen 2010 ONSC 2823, 2010 CarswellOnt 5639 (Ont. Master) at ¶ 23: Photographs of parties posted to their Facebook profiles have been admitted as evidence relevant to demonstrating a party's ability to engage in sports and other recreational activities where the plaintiff has put his enjoyment of life or ability to work in issue: Cikojevic v. Timm, 2008 BCSC 74 (B.C. Master), para. 47; R. (C.H.) v. R. (0.D.), 2008 NBQB 253 (N.B. Q.B.), paras. 54 and 61; Kourtesis v. Joris, [2007] O.J. No. 2677 (Ont. S.C.J.), paras. 72 to 75; Goodridge (Litigation Guardian of) v. King (2007), 161 A.C.W.S. (3d) 984 (Ont. S.C.J.) [2007 CarswellOnt 7637 (Ont. S.C.J.)], para. 128. In one case the discovery of photographs of a party posted on a MySpace webpage formed the basis for a request to produce additional photographs not posted on the site: Weber v. Dyck, [2007] O.J. No. 2384 (Ont. Master).

16 [2007] O.J. No. 5511.

17 Ibid at ¶ 10.

Madam Justice Rady was persuaded that the production of such documents and photographs satisfied two purposes: the documents sought could be used by the defendant in order to impeach the plaintiffs credibility regarding the impact of the accident on her life, and they might also be useful as a means to assess the value of Ms. Murphy's claim for damages.

As such, Rady J. ordered production of the web pages in question, concluding that relevance was established and that the defendant was not on a fishing expedition:

> It seems reasonable to conclude that there are likely to be relevant photographs on the site for two reasons. First, www.facebook.com is a social networking site where I understand a very large number of photographs are deposited by its audience. Second, given that the public site includes photographs, it seems reasonable to conclude the private site would as well.
>
> On the issue of relevancy, in this case, clearly the plaintiff must consider that some photographs are relevant to her claim because she has served photographs of her prior to the accident, notwithstanding that they are only "snapshots in time".18

There have been cases in which courts have held that relevance was not established and, as a result, production and preservation orders were refused. In *Shuster v. Royal & Sun Alliance Insurance Co. of Canada*," the plaintiff sued her insurer to recover compensation for injuries she suffered in an automobile collision. The plaintiff alleged that her injuries compromised her ability to work and to participate in social and recreational activities. After examining the plaintiff for discovery, the defendant learned that she had a private Facebook account with access granted to 67 friends.

The defendant's motion for production of the documents from the webpage was denied by Justice Price. The plaintiff did not disclose the contents of her Facebook account in her Affidavit of Documents and the defendant argued the plaintiff must have violated her obligation to disclose.20 As per the *Rules of Civil Procedure*, all parties in a litigation have an obligation to disclose all relevant documents to the other side.21 However, Justice Price held that the mere fact that the plaintiff possesses a Facebook account does not allow one to assume that it contains relevant information as to the claim.22

> In reviewing Leduc v. Roman and Murphy v. Perger, Justice Price held that:
>
> [w]hat is determinative, in my opinion, when drawing an inference as to whether there is relevant information in the private pages of a litigant's Facebook account is whether there is relevant information in their public profile.23

---

18 Ibid., at ¶ 17-18.

19 2009 CarswellOnt 6586, 83 C.P.C. (6th) 365 (Ont. Sup. Ct.).

20 Ibid. at ¶ 30-31.

21 Ibid. at 29.

22 Ibid. at ¶ 39.

23 Ibid. at ¶ 37.

Justice Price concluded that the plaintiff's privacy interests would be respected unless the defendant established a legal entitlement to such information.24 Justice Price held that there is a presumption that the failure to include Facebook documents in her Affidavit of Documents means that these documents did not contain relevant information. However, the defense may rebut the presumption by cross-examining the Plaintiff on her Affidavit of Documents to ensure that she has complied with her disclosure obligations.25

Location of Electronic Evidence

As existing technology matures, and new technologies emerge, litigators are faced with an ever-expanding list of media as potential sources on which relevant electronic evidence may reside. Examples of such devices include personal digital assistants ("PDAs"), i.e. Palm Pilot, Pocket PCs or Blackberry devices, digital audio devices, mobile phones, memory keys, laptop and personal computers, servers, data tapes, external hard drives, compact disks and DVDs.26 This diverse sampling of electronic devices capable of storing data re-enforces the notion that counsel ought to think carefully about what potential sources of relevant information may exist in a given case.

Portable storage devices primarily conceived for one purpose may also be used to store other types of data, and in the process become treasure troves of valuable information. Such dual use is made possible through the implementation of a computer protocol referred to as USB Mass Storage Class27, which enables a portable storage device to effectively act as a hard drive interfaced to a personal computer through a universal serial bus port. An example of such a device is the iPod, which, while primarily associated with the storage and playback of music, may also been used to store data. As such, and not unlike a memory key,28 it too can be used to misappropriate confidential information. The type of data that can be stored on such portable digital devices is virtually unlimited. The phenomenon of misappropriating confidential information through the use of a portable digital storage device has become known as "pod slurping"29.

Identifying Sources of Electronic Evidence

Maximizing the potential benefit of electronic evidence, on the one hand, and meeting one's preservation obligations, on the other, requires a basic understanding of the various types of data that exist.

---

24 Ibid. at ¶ 53.

25 Ibid. at ¶ 40.

26 Cindy Clarke and Peter Vakof, "Understanding Types and Sources of Electronic Evidence", Osgoode Hall Law School — Professional Development — Obtaining, Producing and Presenting Electronic Evidence (June 10-11, 2009) Materials at Tab 1. See also Kim, Tae, "E is for evidence", online: CA Magazine <http://www.camagazine.com/archives/print-edition/2004/january-

febru /re lars/cama azine15012.as x>.

27 For a technical overview of this protocol, see:

http://www.usb.org/developers/devclass docs/usb msc overview 1.2.pd.f.

28 See for e.g. Factor Gas Liquids Inc. v. Jean, 2008 CanLII 15900 (ON S.C.) at para.8, a case in which an employer accused its former employee of misappropriating confidential information through the

Active data, arguably the most readily accessible, consists of "data that is currently used by the parties in their day-to-day operations."" Practically speaking, active data includes any documents created by word processors, spreadsheets, email or any files created by the operating system. Such data usually must be viewed within an application (computer program) to be useful. By contrast, archival data "is data organized and maintained for long-term storage and record keeping purposes.„31 Typically such data results from the periodic transfer of data to other media such as CDs or network servers. Different still is backup data, which specifically "refers to an exact copy of system data [and] serves as a source for recovery in the event of a system problem or disaster."32 This type of data is often not readily available to system users and may be stored off site. Accessing such data sometimes "requires special (and sometimes expensive) intervention before it is "readable"."33

Yet there are other types of data that, while accessible, are not readily visible by an end user. While it may be more convenient to review paper documents, paper documents do not contain the "hidden" information found only electronically, access to which can prove invaluable in the context of litigation. Colloquially referred to as "hidden data", there are essentially three sub-species within this broad category. The first is metadata, which consists of "information on file designation, creation and edit dates, authorship, and edit history, as well as hundreds of other pieces of information used in system administration."34 Residual data consists of information remaining on a computer system after document deletion. Files are not completely deleted until overwritten by other files. Replicant data "is created when a software program, such as a word processor, makes periodic back-up files of an open file [...] to facilitate retrieval of the document where there is a computer malfunction."35 Upon the creation of a new backup file, the existing file is deleted or tagged for re-use.

It should be noted that, despite the availability of data such as residual data, archival data, or backup data, the principle of proportionality will limit the instances where such data must be produced.

---

clandestine use of a USB memory key during the final stages of his employment. See also http://www.practicepro.ca/practice/pdf/ManagingSecurityPrivacy.pdf at p.33.

29 See Shane Shick, "Be afraid of the file-slurping iPod", Online: Globe and Mail <http://www.theglobeandmail.com/report-on-businessiarticle812678.ece> and GFI Whitepaper "Pod Slurping — An easy technique for stealing data", Online: GFI <http://www.gfi.com/whitepapers/pod-s1 • in -an-eas -techni • ue-for-stealin • -data. df >.

39 Task Force on the Discovery Process in Ontario, Guidelines for the Discovery of Electronic Documents in Ontario, Supplemental Report, October 2005 at p.5 [Ontario Guidelines].

31 Supra note 30 at p.5.

32 Supra note 30 at p.5.

33 Supra note 30 at p.5.

34 Working Group 7, The Sedona Canada Principles — Addressing Electronic Discovery, January, 2008 at p.3, online: University of Montreal <http://www.lexum.umontreal.ca/e-discovery/documents/SedonaCanadaPrinciples01-08.pclf> [Sedona Principles].

35 Supra note 30 at p.6.

Proportionality dictates that discovery of relevant information available from multiple sources should be limited to sources that are the most convenient, least burdensome and/or least expensive.36 In other words, only reasonably accessible and non-duplicative information in support of plausible causes of action should be requested or produced. On the other hand, where there is evidence that the only source of potentially relevant information is not readily accessible (as a result of the organization's poor record keeping practices, for example), the proportionality principle should not assist the party in avoiding their production obligations. A court may choose to limit discovery of inaccessible media, however, if the information stored on the tapes can be obtained from more accessible sources, such as hard copy records, testimony, or non-party discovery. For example, if the producing party can easily produce hard copies of emails, that party should not have to incur the costs of restoring back-up tapes containing the same e-mails, unless the electronic version of the emails contains information relevant to the issues of the matter not available in the hard copy (such as non-visible email metadata.37

To further illustrate the impact that the principle of proportionality may have on discovery, consider the following scenario. In response to a request for the production of e-mails of a former employee, the responding party explains that the e-mail stores of a former employee are no longer available in active storage but that the other custodians would have copies of e-mails they sent to or received from that employee. In such a scenario, the court, in responding to a request made by the opposing party for production of the back-up tape, would be unlikely to order production based on the principle of proportionality if there was evidence that the emails could be obtained from the other custodians. In this case, it may be necessary to sample the other custodians' mailboxes and the backup tapes to confirm that the emails do, in fact, reside in the other custodians' mailboxes. In addition to the fact that the information could be obtained more easily and conveniently from another source, there is low probability of finding additional relevant information in the backup tapes that contain the former employee's mailbox such that the marginal utility of this course of information does not warrant its cost.

While it has long been settled that parties have the obligation to preserve relevant electronic data stored on a stable medium38, for example, a hard drive, whether the same duty extends to such data stored in a computer's dynamic memory, or Random Access Memory ("RAM"), is unclear. This is hardly surprising when one considers the sheer volume of data processed through RAM and the ephemeral nature of data "stored" in RAM.

This very issue was addressed by the United States District Court for the Central District of California in *Columbia Pictures Industries v. Bunnell*39 . In this case, the Plaintiff brought a copyright claim against the Defendants, operators of the website TorrentSpy, on the basis of contributory infringement, secondary infringement and inducement or hosting a web site through which end users

---

36 Sedona Commentary, supra, note 8 at p. 9.

37 Ibid, at p. 10.

38 See supra, note 34, specifically principle 3 and accompanying commentary.

39 2007 WL 2080419 (C.D.Cal. May 29, 2007) [TorrentSpy].

downloaded Torrent files.4° Through a motion to compel discovery, the Plaintiff sought to require the Defendants to preserve and produce data logs containing the IP addresses of its users, files requests, and corresponding dates and access times. This information was stored temporarily in the dynamic access memory of TorrentSpy's servers for approximately six hours. The Plaintiff argued that this information was highly relevant on the basis that "a case cannot be made against a website alleged to have engaged in secondary/contributory infringement because such logs are "essential" to finding direct infringers."41 The Defendants resisted the Plaintiff's motion on the basis that the data in question did "not constitute electronically stored information [...] because the data has never been electronically stored on their [the Defendants'] website or in any medium from which data can be retrieved or examined or fixed in any tangible form, such as a hard drive."42 To resolve this issue, the Court looked to jurisprudence in another context, that of the *Copyright Act*43 , in which it was held that data copied into RAM was held to be "fixed", albeit temporarily, and concluded that for the purposes of Rule 34(a) of the *Federal Rules of Civil Procedure*44 , the data qualified as electronically stored information ("EST").

None of the Defendant's other arguments were able to sway the Court in its favour. For example, an issue arose with respect to the fact that the data was being stored on third-party servers in Amsterdam, and therefore outside of the Defendant's possession, custody or control. The Court resolved this issue on the basis of the established legal principle of deemed possession, custody or control, which applies where a party has actual possession, custody or control of data. The Court also rejected other objections to the Plaintiff's request premised on the financial and logistical burdens of recording the data, privacy issues, loss of good will, and conflict of law issues"'. The Court did, however, qualify its holding that the server log data was the proper subject matter of a preservation order in this particular case due to the its high probative value, a lack of alternative means of obtaining this data, and the Defendants' failure to establish undue burden or economic hardship.

Although the Defendants subsequently brought a motion for review of the Magistrate's decision46, it was ultimately denied. In response to this denial, the Defendants proceeded to deny U.S. internet users access to their web site presumably on the premise that "if there are no users within the jurisdiction, there may be no relevant server log data for defendants to preserve or produce in this case."47

---

49 For more information on the nature and use of BitTorrent technology, see http://www.bittorrent.com.

41Supra note 39 at p. 11, para 15.

42 Supra note 39 at p. 13, para 2.

43 90 Stat. 2541 (1976).

44 F.R. Civ. P. 34(a).

43 For a more fulsome discussion of the conflict of law issues that arose in this decision, see LexisNexis, "Columbia Pictures v. Bunnell: Foreign Privacy Laws vs. U.S. Discovery Obligations", online: LexisNexis <http://law.lexisnexis.com/litigation-news/articles/article.aspx?groupid=e0SqfLggRQQ=8Larticle=G3e/MZEnBrM=>.

46 See Columbia Pictures, Indus. v. Bunnell, 2007 U.S. Dist. LEXIS 63620 (C.D. Cal. Aug. 24, 2007).

47 Supra note 45.

The Plaintiffs would go on to successfully bring a motion for "terminating sanctions" in response to the spoliation of evidence by the Defendants. This decision is currently pending appeal before the United States Court of Appeals for the Ninth Circuit. We have been unable to locate an appeal decision and have assumed that this case has been settled.

In the aftermath of the preliminary ruling with respect to the preservation of data stored in RAM, several concerns have been raised. For example, if applied broadly, the decision could impose an enormous burden on litigants already subject to expensive discovery requirements, and could intrude on the privacy rights of litigants and third parties." Yet the conceptual soundness of the ruling has been questioned on the basis that:"

> The district court's interpretation effectively reads the "S" out of "ESI." Information in RAM is not "stored" in the sense intended by Rule 34, which refers to information stored in a "medium," see FED. R. CIV. P. 34(a), not information in volatile memory.

While from a technical standpoint the notion that data held in RAM is not effectively "stored" may seem intuitively appealing, it is unlikely that the argument could be successfully made in Ontario. The *Rules of Civil Procedure*5° define the term "document" very broadly as encompassing "data and information in electronic form."51 For their part, the *Sedona Canada Principles* provide some guidance in this regard through the adoption of a remarkably expansive definition of electronic information, being "virtually any information that is stored on a computer or other electronic device [provided that it] can be read through the use of computers or other digital devices."52 RAM is specifically enumerated as a medium from which electronic information may be accessed. Thus, subject to other well-established principles53, data stored in RAM is potentially subject to preservation and production obligations in the course of litigation conducted in the province of Ontario.

---

48 Etish, Scott J., "RAMing New ESI Preservation Obligations Down Litigants' Throats - Columbia Pictures Industries v. Bunnell, 2007 WL 2080419 (C.D.Cal. May 29, 2007)", online: Gibbons http://www.gibbonslaw.com/news publicationstarticles.php?action=display_publication&publication id=2 210>.

49 Kwun, Michael, "BRIEF AMICI CURIAE OF THE ELECTRONIC FRONTIERFOUNDATION, THE CENTER FOR DEMOCRACY & TECHNOLOGY, AND PUBLIC KNOWLEDGE IN SUPPORT OF NEITHER PARTY, URGING VACATUR OF THE AUGUST 24, 2007 ORDER DENYING DEFENDANTS' MOTION FOR REVIEW", online: Electronic Frontier Foundation < http://www.eff.org/filesifilenodeitorrentspy/20090212%20Amicus%20Brietpdf> at p.7.

5° R.R.O. 1990, Reg. 194 [Rules of Civil Procedure].

51 See the definition of "document" in Rule 30.01(1)(a) as well as the definitions of "document" and "electronic" in Rule 1.03, ibid. See also the definition of "document" in s.222(1) of the Federal Court Rules, SOR/98-106, which includes any device on which information is recorded or stored.

52Supra note 34 at p.1 under the heading "What is Electronic Discovery ("e-discovery")?", and Principle 1 and accompanying commentary.

Benefits and Risks of Metadata

Metadata is "evidence, typically stored electronically, that describes the characteristics, origins, usage and validity of other electronic evidence."54 Metadata is broken down into two basic categories: application metadata and system metadata, the fundamental difference being that in the case of the former, the data resides with the file to which it relates, whereas with respect to the latter, it is "stored externally and used by the computer's file system to track file locations and store demographics about each file's name, size, creation, modification and usage."55 The scope of a document's metadata is broad, encompassing information on "file designation, creation and edit dates, authorship, and edit history, as well as hundreds of other pieces of information used in system administration."56 The primary benefit of metadata is that it provides a party with information that would otherwise be unavailable in paper copy. Indeed, it is for precisely this reason that where one has access to metadata associated with a given document, it is the best evidence. From a practical perspective, the benefit of accessing metadata is that it provides lawyers with information to support or defend their client's cases, streamlines document review, and provides a more complete story about adversaries' documents.

Whether metadata will be of any value to a litigant will be determined by the scope of the issues presented in the litigation. In some cases it may be of no benefit at all. Indeed, much turns on the question of relevance, which at law necessitates that such information "increase or diminish the probability of the existence of a fact in issue"57. In this regard, although different in nature from the document to which it belongs, metadata has been characterized as "part of the substantive content of the document"58 such that if it is "[...] determined that a particular document is relevant, the metadata in relation to such document should be produced."59 At its core, metadata "describes how, when and by whom an electronic document was created, modified and transmitted."6° For example, where the authorship of a document or of a modification to a document is at issue, for instance in a contract dispute, where iterations of an agreement are likely to have been exchanged on several occasions between the parties, metadata and specifically the ability

---

53 i.e. Relevance and Proportionality; See Principle 2 and accompanying commentary, supra, note 34 at p.11 as well as Rule 29.2 of the Rules of Civil Procedure, supra note 50, that speaks specifically to proportionality.

54 Craig Ball, "Beyond Data about Data: The Litigator's Guide to Metadata" online: <http://www.craigball.com/metadata.pdf>.

55 Supra note 54 at p.2.

56 Supra note 34 at p.3. An interesting and less obvious example of metadata occurs with some digital photographs, where a thumbnail of a photograph is embedded within the file. See http://michaelzimmer.org/2006/06/13/the-hidden-photos-within-photos/ for more information.

57 R. v. Grn (2009), 307 D.L.R. (4th) 577 (S.C.C.), at para. 89, citing R. v. Arp, [1998] 3 S.C.R. 339 (S.C.C.), at para. 38.

58 See supra, note 34 at p.3, footnote 11.

59 Hummingbird v. Mustafa (2007), 2007 CarswellOnt 6012 (Ont. Master) at para. 9.

6° Ibid.

to examine the history of changes associated with an electronic document may prove determinative. In short, if "the origin, use, distribution, destruction or integrity of electronic evidence is at issue, the 'digital DNA' of metadata is essential evidence that needs to be preserved and produced."61

The recent decision of *Bishop v. Minichiello*62 provides an example of the unique evidence metadata can provide that could otherwise be unattainable. In that case, the defendant sought the production of the plaintiff's entire hard drive of his family computer in order to determine the period of time the plaintiff spent on Facebook between 11:00PM and 5:00AM each day by obtaining his login/logout information. The information was relevant to the defendant's case in that the plaintiff allegedly suffered a brain injury and claimed that ongoing fatigue prevented him from maintaining employment. The defendants argued that the records from the computer would indicate how much time the plaintiff spent on the web site Facebook each night and was therefore relevant to an evaluation of his past and future employment.

In his analysis, citing the previous B.C. cases of Ireland63 and Park64, Melnick J. determined that:

> Electronic data stored on a computer's hard drive or other magnetic storage device falls within the definition of 'document' under Rule 1(8) of the *British Columbia Rules of Court*, and further that Rule 26(1) requires disclosure of documents relating to any matter in question in the action. The decision as to whether to grant an order requiring production under R. 26(10) is a discretionary one. The court has used its discretion to deny an application for the production of documents in the following two circumstances: first, where thousands of documents of only possible relevance are in question; and second, where the documents sought do not have significant probative value and the value of production is outweighed by competing interests such as confidentiality and the time and expense required for the party to produce the documents. Additionally, privacy concerns should be considered in a determination under R. 26(10), where the order sought is so broad it has the potential to unnecessarily delve into the private aspects of the opposing party's life.65

Melnick J. agreed that metadata is information recorded or stored by means of a device and is thus a document under R. 1(8), as established *in Desgagne*.66 Since metadata is a report of

---

61 Supra note 54 at p.6.

62 2009 B.C.S.C. 358, [2009] B.C.W.L.D. 3473, 69 C.P.0 (61) 344.

63 Ireland v. Low (2006), 2006 BCSC 393, 2006 CarswellBC 1364, 35 C.P.C. (6th) 384 (B.C. S.C.).

64 Park v. Mullin (2005), 2005 BCSC 1813, 2005 CarswellBC 3162 (B.C. S.C. [In Chambers]).

65 Supra note 62, at ¶ 46-47.

66 Desgagne v. Yuen (2006), 56 B.C.L.R. (4th) 157, 33 C.P.C. (6th) 317 (S.C.) at ¶ 29.

recorded data generated by computer software, it is not something created by the user; rather, it is based on what the user does with their computer.67 Since the application in this case was narrow in scope, that is, the defendant wanted access to the plaintiff's hard drive for a specific purpose — to determine the length of time spent on Facebook during the night — and since information elicited on examination for discovery indicated the plaintiff was the only person in the family using the computer during thosehours, Melnick J. held in favour of the defendants and granted the production order." He held that the information sought by the defence may have significant probative value in relation to the plaintiffs past and future wage loss, and value of production was not outweighed by competing interests such as confidentiality and the time and expense required for the party to produce the documents.69

As probative as metadata has the potential to be useful in some circumstances, parties must always be cognizant of the possibility that metadata may be misleading. For example, using word processing templates to create new documents may incorrectly identify the template author as the new document creator. The recording of metadata related to e-mail is fraught with its own inherent flaws, including the inability to account for differences in time zones, and the possibility that such metadata can be manually reset by the user.76 Transferring files to storage media may result in a loss of metadata. For example, metadata such as the document creation date or date last modified or date last accessed could be lost when transferring the file data to a recordable CD.

Many lawyers do not recognize that any subsequent manipulation of a given file, including a simple review of the evidence, however innocuous or inadvertent, may give rise to allegations of spoliation. The inherent fragility of metadata, was acknowledged by the *E-Discovery Guidelines*, which directs parties to discuss the need to preserve or produce meta-data as early as possible.71

From counsel's perspective, ignoring the existence of metadata where electronic documents are being sent to opposing counsel can lead to the inadvertent disclosure of confidential information. Indeed, modern day word processors allow for changes to be tracked or comments to be embedded within a document and these are not always visible to the end-user. While these features may prove indispensible with respect to internal document preparation and review, they may very well contain sensitive and confidential information which, if disclosed, would result in the breach of a lawyer's professional ethical obligation.72 Working from a precedent, as many do for reasons of efficiency, presents a heightened risk of inadvertent disclosure and extra care should be taken to ensure that no residual data remains from the original document. For example, recycling of precedent documents

---

67 Supra note 62, at ¶ 50.

68 Ibid. at If 53-54.

69 Ibid. at If 57.

7° See supra note 34 at p.3, footnote 10.

71 See Principle 7 and accompanying commentary, supra, note 30 at p.13.

72 Lawyers owe their clients a strict duty to maintain confidences unless otherwise authorized by a client or compelled by law, pursuant to Rule 2.03(1) of the Rules of Professional Conduct - see: http://www.lsuc.on.calmedialrpc 2.pdf quite apart from the notion of solicitor-client privilege, a concurrent legal obligation.

can result in inadvertent disclosure of information if care is not taken to strip all residual data from the original document. The potential consequences resulting from inadvertent disclosure can be dire: complaints to professional regulatory bodies resulting in discipline hearings, litigation and potentially being subject toprosecution under the *Personal Information Protection and Electronic Documents Act*73. Some professional regulatory bodies have expressly opined on the respective duties and ethics regarding this very issue. For example, in the State of New York, the New York Bar Association Committee on Professional Ethics has taken the position that:74

> Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in "metadata" in documents they transmit electronically to opposing counsel or other third parties.

An example of the type of inadvertent disclosure of confidential client information contained in metadata follows:75

> An attorney looks in his inbox and finds a long-awaited settlement proposal from opposing counsel attached to an e-mail. The attorney opens the document and hits the print command. While the document is printing, the attorney eagerly looks at the monitor for details. "Good, the settlement figure is probably still too high, but very close to reasonable." The document is quite short, actually. How long could drafting it have taken? Idly, the attorney clicks on the properties tab and sees the document was open on opposing counsel's computer for three hours.
>
> "Wait," the attorney thinks. "Didn't I get that metadata scrubber utility? They said it could be used to look at metadata, too. He locates the icon and clicks on it. In a few moments, he is reviewing the revision history of the document. It looks like several documents were combined and then a lot of deletions were made at the end. The lawyer pulls up a large block of deleted text and begins to read, "Notes. Client is desperate to recover something and not face the PR disaster of receiving nothing at trial. Offer $100K. But get it settled before end of month even if we have to take half that."

---

72 Lawyers owe their clients a strict duty to maintain confidences unless otherwise authorized by a client or compelled by law, pursuant to Rule 2.03(1) of the Rules of Professional Conduct - see: http://www.lsuc.on.calmedialrpc 2.pdf quite apart from the notion of solicitor-client privilege, a concurrent legal obligation.

73 S.C. 2000, c. 5, [PIPEDAJ. See Tana Christianson, "Meta Data Alert", Communique (January, 2004), online: Law Society of Manitoba.

<htt.://www.lawsociet .mb.ca/communi•ue/communi ue an04.htm#meta data>.

74 New York State Bar Association — Committee on Professional Ethics — Opinion 782 — 12/8/04, online: New York State Bar Association.

<http://www.nysba.org/AM/Template.cfm?Section=Ethics Opinions&CON I ENTID=6871&TEMPLA 1 E,

=/CM/ContentDisplay.cfm>. The District of Columbia Bar has adopted a similar stance on this issue; see http://ww.dcbar.org/for lawyers/ethics/legal ethics/opinions/opinion341.cfm. For other American examples see infra note 57.

75 Jim Calloway, "Metadata — What Is It and What Are My Ethical Duties?" online: LLRX.com <http://www.11rx.com/featuresimetadata.htm>.

Metadata risks can be mitigated. Documents may be stripped of their metadata prior to being exchanged through the use of tools found within the software by which they were created, and parties may use more appropriate file formats for exchanging documents.76 Much like in the case of a document retention policy, organizations are well-advised to approach the treatment of metadata in a thorough and systematic manner77

Omnipresent Nature of Electronic Information

The advent of global networking and the ease with which data may be accessed and stored across networks transcending political borders has raised issues of jurisdiction, location and ownership of information. The case of *eBay Canada Limited v. Canada (National Revenue)*78 is instructive. Here, an ex parte order was made by the Federal Court compelling eBay Canada Limited and eBay CS Vancouver Limited ("eBay"), both effectively subsidiary companies of eBay Inc., their American parent, to provide information with respect to a segment of its customers to the Minister of National Revenue. The order was made pursuant to s.231.2 of the *Income Tax Act*79, which enables the Minister to require 'any person' to provide 'any information'. The request must be made 'for any purpose related to the administrative enforcement of this [Income Tax] Act'.8°.The information in question, which consisted of both account information and merchandise sales information relating to Canadian users of the website who qualified as "PowerSellers"81, was stored remotely on servers belonging to eBay Inc. located in San Jose, California. Pursuant to s.231.2(5) of the *Income Tax Act*, eBay applied to have the order reviewed. Thus, the narrow issue was whether s. 231.2 required a Canadian resident to provide information accessible in Canada but stored in data facilities owned by another party located outside Canada."

The technological reality compelled the Court to conclude that such an order could be made. The Applicants argued that given the location of the stored information, which effectively amounted to a "foreign source", the more restrictive s.231.6 was applicable, which would not have permitted the blanket request that was made. The Court rejected the formalistic argument premised on physical location and instead focused on ease of access, reasoning that:"

---

81 For more details regarding this program, see htAx//pages.ebay.com/help/sell/sell-powersellers.html.

76 For software bundled with the Microsoft Office suite, see: http://office.microsoft.com/en-us/help/ha010776461033.aspx. For a practical guide to converting Microsoft Word Documents to Adobe Portable Document Format ("PDF"), see http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf.

77 Security Best Practices — Document Security, online: Metadatarisk.org <http://www.metadatarisk.org/best practice/best prac overview.htm>.

78

eBay Canada Ltd. v. Minister of National Revenue (2007), 285 D.L.R. (4th) 488 [eBay] (Federal Court).

79 R.S.C. 1985, c. 1, as amended [Income Tax Act].

80 Supra note 78 at para. 19.

82 Supra note 78 at para. 16.

> Such information cannot truly be said to "reside" only in one place or be "owned" by only one person. The reality is that the information is readily and instantaneously available to those within the group of eBay entities in a variety of places. It is irrelevant where the electronically-stored information is located or who as among those entities, if any, by agreement or otherwise asserts "ownership" of the information.

The Court's reasons underscore the important distinction drawn between the message, or substantive content of the data, and the medium upon which it is stored. The Court reasoned that: "[i]t is not determinative of the issue that the electronic apparatus storing the information which eBay Canada accesses is outside Canada. The information can be summoned up in Canada and for the usual business purposes of eBay Canada."84 Thus, access to and actual use of the information, rather than its physical location, was pivotal to the Court's decision to uphold the impugned order. The interesting implication of this decision is that, at least for the purposes of s. 231.6 of the *Income Tax Act*, information stored on a device physically outside of Canada's borders is, in certain circumstances, not "foreign-based" at all. The decision was later unsuccessfully appealed, with the Federal Court of Appeal adopting a similar view on the issue:85

> [...] it makes no sense in my view to insist that information stored on servers outside Canada is as a matter of law located outside Canada for the purpose of s.231.6 because it has not been downloaded. Who, after all, goes to the site of the servers in order to read the information stored in them?

The issues of ownership and jurisdiction raised in *eBay Canada Limited* will become even more prominent with the rise of cloud computing. Cloud computing refers to internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like electricity. It is likely that companies using cloud computing may find themselves using hardware and software that are in different countries from their own physical locations, thus creating additional barriers to the accessibility of such ESI.

Where to start and what to collect before taking the electronic journey

Taking appropriate measures with respect to data retention and preservation long before conflict arises is critical to avoiding the imposition of potentially serious judicial sanctions." It is also the most logical place to start. Being proactive in this regard involves developing and implementing procedures and policies for preserving and producing potentially relevant ESI, and establishing processes to identify, locate, retrieve, assess, preserve, review and produce data87 as well as a policy which establishes routine retention and destruction guidelines.

---

83 Ibid. at para. 23.

84 Ibid. at para. 24.

85 See eBay Canada Ltd. v. Minister of National Revenue (2008), 53 B.L.R. (4th) 202 at para. 48.

86 See Principle 11 and accompanying commentary, supra, note 34 at p.36.

87 Supra, note 34 at p.13 under heading "Comment 3.b. Preparation for Electronic Discovery Reduces Cost and Risk".

While the development of an appropriate records retention policy will vary from case to case, a systematic approach toward its development is ideal. For example, how long to keep a document, when and how to store the document, and how to dispose of the document, will depend on the type of document. Legal and regulatory requirements may also dictate what documents must be kept and for how long. The following inquiries should therefore be made in the course of developing a document retention policy:89

a) Is there a legal requirement for keeping the document? Legal requirement include federal and provincial laws concerning various regulated matters, such as employment records, health and safety records, tax records, etc;

b) After the item is used for its intended purpose, what other purpose could it serve? Could it be used to support or oppose a position in an investigation or lawsuit? Could it support a tax deduction or balance sheet item? Could it support or explain a business decision?

c) What is the consequence of not being able to locate the document? If the document was destroyed pursuant to a records-retention program and no threat of litigation was pending at the time, the issue will be how reasonable the document retention/destruction program was. If the document is central to a lawsuit and is suddenly destroyed after litigation is commenced or threatened, the presumption will be that the destruction was accomplished deliberately.

d) Can the item be reliably reproduced elsewhere if needed? Is the information available from another database or source?

e) Once the possible use of a particular item is determined, the question becomes how long to retain the document. This question is answered by taking into account the relevant statutes of limitations, being the time period within which a lawsuit must be commenced for a particular claim after the basis for the claim is discovered, as well as any retention periods stipulated by law, such as income tax statutes.

Outside of the litigation arena, an effective document retention policy can also reduce the burden/costs of storing irrelevant and obsolete documents, can assist in the identification and retrieval of documents and can facilitate the review of a large number of documents in an efficient manner. Another equally important purpose is to ensure that relevant and potentially useful records are retained which serves to preserve corporate memory and enhance productivity. Central to the preservation obligation is the concept of the litigation hold, which may alter a pre-existing records retention policy. The underlying premise of the litigation hold is that parties to an action are obliged, from the moment litigation is contemplated or threatened, to take reasonable and good faith steps to preserve relevant ESI.9° The litigation hold allows a party to meet its preservation obligations through

---

88 Ibid.

89 Barbara Weil Gall, "Document Retention Policies: Legal Reasons to Keep E-mail, Web-Pages and Other Records, online: Gigalaw <http://www.gigalaw.com/articles/2000/-all/gall-2000-09-all.html>.

9° See Principle 5, supra note 30 at p.12.

the adoption of a protocol which stops normal course deletion and alteration of information."91 The successful execution of a litigation hold requires the co-operation of a number of groups of individuals, including IT and records management personnel along with key employees. The co-operative effort of this group will determine relevancy and the necessary preservation steps.

From a practical perspective, successfully implementing the litigation hold requires a substantial amount of preliminary investigative work, which assists in establishing the outer boundaries of a party's preservation obligation. In order to make most efficient use of resources and contain costs, a party should first determine, by reference to the pleadings among other things, *who the key players are* within its organization, and further, *what the material timeline is*. Identifying these two key pieces of information will allow the party to focus its efforts and shape the breadth of the litigation hold in a manner that makes it manageable and effective.

As contemplated by the requirements of Rule 29.1 of Ontario's *Rules of Civil Procedure*, parties should discuss what information is really relevant, material and probative of the issues in dispute. Not all sources are going to be as valuable as others, and some will be more expensive to produce because they are difficult to process or because they result in large volumes of duplicative and irrelevant information that must be culled and reviewed. At the initial discussion, parties should agree on steps required to preserve information.

Before the actual collection, parties should agree on how to focus the search for relevant information to reduce the quantity of irrelevant information. Parties need to balance the need for particular forms of ESI that are relevant and material to the issues in dispute against the cost of retrieving it. As such, parties should inform themselves of the costs involved in retrieving the information being sought by the opposing party.

They may agree on the names of key custodians and restrict the collection to specific date ranges; they may go further and agree on what kinds of information can be excluded from production as being clearly irrelevant, such as e-mails from and to individuals known not to have been involved in any way with the events. Finally, they may agree to phase production so that documents meeting narrow search criteria will be examined by both sides to see what kinds of information is missing and still required.

The need for collaborative conduct at the discovery stage stems from the recent changes to the *Rules of Civil Procedure* emphasizing proportionality as a key consideration in the discovery process and the push for a change in legal culture by the judiciary given the exponential growth of information.92 In many cases, it is cost-prohibitive, if not impossible, to uncover and produce every

---

91 Susan Wortzman, "Spoliation, Litigation Holds and Preservation Orders — The New E-Discovery Guidelines", (2005) OBA CLE — Electronic Discovery and the New ED Guidelines — A Roadmap for Dealing with Electronic Information at tab 6.

92 Sedona Commentary, supra, note 8 at p. 4.

potentially relevant document. Parties and their counsel should accept a change from all potentially relevant information to that which is truly necessary to the resolution of the conflict.93

With respect to isolating key individuals, the following are examples of steps that should be taken:94

a) Ascertain how each individual uses his or her computer and include those individuals' secretaries and assistants. (Documents drafted by a key party or witness may be stored on an assistant's computer).

b) Ascertain the identity of people who have access to relevant documents including any third parties who may have been provided with copies.

c) Determine the computer resources to which the individuals have access including the type of connections that exist between computer resources and others in the organization including e-mail and local area networks.

Having made these preliminary determinations, there are a number of steps that remain to be completed in order to carry out the litigation hold. Broadly speaking, in a typical case, at this point a party would proceed to:95

(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 ESI;

(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 ESI in the ordinary course of business.

---

92 Sedona Commentary, supra, note 8 at p. 4.

93 With respect to narrowing the scope of relevant information, see the change to the wording of Rule 30.02(1) effective as of January 1, 2010 where the reference to "relating to any mater in issue" was replaced with "relevant to any matter in issue". This change, recommended by Justice Osborne, was intended to replace the "semblance of relevance" test with a simple relevance test.

94 Karen Groulx, "Newest Technology Advances in E-Discovery that Could reduce Cost and Time", Insight Program, June 21, 2007 (Citing Alan Gahtan, Electronic Evidence, 1999, pp. 31-32).

95 See Ontario Guidelines commentary under Principle 5, supra note 30 at p.12. See also Brad Harris, "Eight Steps to Defensible Legal Holds", online: Fios, Inc. <http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discovery-article.aspx?id=50 1&cid=enlc-090212>.

Determining the types and sources of data that a party is obligated to preserve while subject to a self-imposed litigation hold is accomplished through the relevance inquiry, which limits the scope of the obligation to preserve documents. In this respect, preservation obligations for ESI are no different from preservation obligations for conventional paper documents. Succinctly put, "[a] party is under a duty to preserve what he knows, or reasonably should know, is relevant in an action."96 What is relevant in a given case, the facts in issue, is determined by reference to the "substantive law relating to the particular [...] cause of action",97 bearing in mind that "[i]n a civil case, the facts in issue are established by the pleadings".98 In *Northwest Mettech Corp. v. Metcon Services Ltd.,*99 it was held that the plaintiff, who sought to obtain production of the defendant's hard drive, which contained data both relevant and not, was only "entitled to production of only the relevant electronic data which is resident on that hard drive"166, and not the drive itself.

IT personnel should be consulted in determining where relevant ESI may reside. They can provide such information regarding what systems are in place, the back-up procedure, the document and information management policies that are in place, etc. Through the use of a "data map", information regarding the type of ESI maintained by an organization and its location can be obtained. A data map is a visual reproduction of the ways that ESI moves throughout organizations, from the point of its creation to its ultimate destruction as part of the organization's information management and document retention program. In addition, the use of "early case assessment" software tools allows users to look at electronic records prior to extracting them and to select the data at source based on date filters and custodian search filtering which decreases the volume of ESI for further processing and therefore the processing costs.

To assist a party in defining its preservation obligations, principles 3 and 4 of the *Ontario Guidelines* discuss how the notion of relevance should apply to e-discovery in order to determine the types of electronic information subject to discovery, and therefore assist in defining the substance and scope of the litigation hold.

Principle 3 states:

> "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 be preserved."101

---

96 Doust v. Schatz (2002), 32 R.F.L. (5th) 317 (Sask. C.A.) at para. 27.

97 Alan W. Bryant & Sidney N. Lederman & Michelle K. Fuerst, The Law of Evidence in Canada, 3rd ed. (Toronto: Lexis Nexis Canada Inc., 2009) at p.52. See also Professional Institute of the Public Service of Canada v. Canada (Attorney General) (2005), 2005 CarswellOnt 7981 (Ont. S.C.J.) at para.41.

98 Ibid. at p. 54.

99 Northwest Mettech Corp. v. Metcon Services Ltd. (1996), 1996 CarswellBC 1889 (B.C.S.C.) [Metcon].

100 Ibid. at para. 10.

101 Ontario Guidelines, supra note 30 at 11.

To assist a party in defining its preservation obligations, principles 3 and 4 of the Ontario Guidelines discuss how the notion of relevance should apply to e-discovery in order to determine the types of electronic information subject to discovery, and therefore assist in defining the substance and scope of the litigation hold.

Principle 3 states:

> "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 be preserved."101

Principle 4 continues:

> "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."102

Where they exist in both formats, documents need to be preserved in both paper and electronic form, for "Canadian courts have typically held that the discovery of documents requires disclosure of documents in electronic form when paper form is not sufficient."103 This principle emerges from the case *Cholakis v. Cholakisla*4, which involved a dispute between brothers in which the plaintiffs complained that the defendant directors failed to manage a company in a reasonable and competent manner, the issue of whether paper-based production was adequate arose. In this case, accounting information was produced by the defendants for the plaintiff, who in turn sought further production of accounting data on a computer disk. It was ordered by a Master that the defendants produce accounting software along with accounting data that had been or would be produced in paper on a floppy disk. On appeal from this order, the basis for the defendant's objection was that this information had already been produced in paper form. The plaintiff took the position that the information stored on the computer would allow him to perform certain accounting functions much more efficiently than having to input a massive amount of data from paper documents. In citing *Reichman v. Toronto Life Publishing Co. (No. 2)*105, the Court concluded that the information stored on the disk came within the definition of a "document" and as it contained relevant information, it was therefore producible. The Court further stated that "[t]he interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."1°6

---

102 Ibid.

103 Todd J. Burke & Glenn Smith, "A Survey of E-Discovery Case Law in Canada", online: Gowlings <http://www.gowlings.com/resources/PublicationPDFs/BurkeT ASurve_yE-DiscovervCaseLaw.pdf>.

104 Cholakis v. Cholakis (2000), 2000 CarswellMan 7 (Man. Q.B.) [Cholakis].

105 Reichman v. Toronto Life Publishing Co. (No. 2) (1988), 66 O.R. (2d) 65 (H.C.J.) [ReichmannJ.

106 Supra, note 104 at para. 30.

The above decision underscores the importance of meeting with opposing counsel early on in litigation to discuss and agree on the format of production.107 In fact, the manner by which the information will be produced is one of the factors the parties must include in their discovery plan as mandated by the *Rules of Civil Procedure*l°8

Admissibility of Electronic Evidence

Notwithstanding its peculiar characteristics, electronic evidence is subject to the same evidentiary rigors as its paper-based counterpart. Electronic evidence, as with all other evidence, must be both material and relevant to the issues as defined by the pleadings, must not be subject to any other exclusionary rule, and must ultimately possess greater probative value than prejudicial effect in order to be received109. Nevertheless, there are some important differences with respect to how certain basic evidentiary legal principles are applied in the context of electronic evidence, largely the consequence of statutory amendment to the common law. Evidentiary issues, which arise with respect to the admissibility of documentary evidence, of which electronic evidence is a species, generally fall into three different categories, and arise because: 11°

> First, it is usually hearsay, rather than the direct testimony of a live witness under oath and available for cross-examination, which is the paradigm of good evidence in our court system. Second, such evidence needs to be authenticated, that is identified in some authoritative way. Third, documents are subject to the "best evidence" rule, which generally requires that original documents be presented to the court, and that a good explanation be given if copies are to admitted instead.

Discoverability of a document, electronic or otherwise, does not ensure its admissibility. A document that must be disclosed to a party adverse in interest may not necessarily be admissible in a judicial proceeding. Something that constitutes a "document" under the Rules is not necessarily admissible evidence. This proposition is supported both by precedent", which has held that "the test for relevance

---

107 See Justice C. Campbell's endorsement of the Discovery Plan agreed to by the parties in Enbridge Pipelines Inc. v. BP Canada Energy Company, 2010 ONSC 3796, where Justice Campbell commended counsel for the responsible and cooperative manner in which they achieved agreement on a Discovery Plan. Justice Campbell incorporated the Discovery Plan into an Order and attached it as an appendix to the decision.

1°8 See Rule 29.1.02(3) of the Rules of Civil Procedure, supra note 8.

109 This is known as the exclusionary discretion of the court, a process by which a judge considers a piece of evidence's "[...1 reliability and the strength of the inferences it leads to against the costs presented by such evidence, including things as diverse as the practicalities of its presentation, the fairness to the parties and to witnesses, and the potentially distorting effect the evidence can have on the outcome of the case." See David M. Paciocco and Lee Stuesser, The Law of Evidence, 4th ed. (Concord: Irwin Law, 2005) at p.23.

10 John D. Gregory, "Canadian Electronic Commerce Legislation", Banking & Finance Law Review, June 2002, online: Gregory/Horton Home Page <http://www.euclid.ca/bflr2002.pdf>.

for documentary disclosure on discovery is broader than the test of relevance for admissibility" 2, and statute", which expressly stipulates that disclosure or production of a document is not tantamount to an admission of the document's relevance or admissibility.

It is difficult to apply historical common law evidentiary principles to ESI, when unlike paper documents, ESI can be easily manipulated and there is no "original" document. For example, authentication becomes problematic.

The *Uniform Electronic Evidence Act*114 ["UEEA"] was drafted in response to these conceptual difficulties. The other impetus for the drafting of the UEEA was the reality that "Canadian courts have not always kept these notions [hearsay, authentication and the best evidence rule] separate in their decisions"115, which has led to uncertainty and the inconsistent application of existing legal principles. The rules of evidence addressed in the UEEA involve the authentication of electronic documents, as well as the application of the traditional common law best-evidence rule. The UEEA does not deal with hearsay evidentiary issues. The Uniform Law Conference of Canada ("ULCC") was of the opinion that electronic evidence did not require changes to the hearsay rules. Thus, while conventional law with respect to authenticity and the best evidence rule subsequently were adapted to better suit electronic evidence, the conventional hearsay approach continues to apply to electronic evidence.

While the UEEA does not bind federal or provincial governments, both the federal and provincial government in Ontario have since incorporated similar provisions in their respective statutes.116 Provisions of the UEEA were adopted by the Federal Government in 2000 by way of Part III of PIPEDA, which consisted of amendments'" to the Canada Evidence Act118 . These amendments, which sought to "clarify how the courts would assess the integrity of an electronic document introduced as evidence"119 came into force in 2003. In similar fashion, Ontario has

iii See Bensuro Holdings Inc. v. Avenor Inc. (2000), 186 D.L.R. (4th) 182.

112 Professional Institute of the Public Service of Canada v. Canada (Attorney General) (2005), 2005 CarswellOnt 7981 (Ont. S.C.J.) at para.36.

113 See Rule 30.05 of the Rules of Civil Procedure, supra note 9, which precludes this possibility.

114 Uniform Law Conference of Canada, Uniform Electronic Evidence Act (1998), online: Uniform Law Conference of Canada <httwww.ulcc.ca/en/us/index.cfm?sec=1ctsub=1u2>.

115 Supra note 110 at p.21.

116 The provisions of the UEEA would be adopted by the federal government in addition to six provinces.

117 Sections 31.1 to 31.8.

118 R.S.C. 1985, c. C-5 [Canada Evidence Act].

119See Legislative Summary, Bill C-6: Personal Information Protection and Electronic Documents Act online: Library of Parliament — Parliamentary Information and Research Service <htt ://www2 arl. c.ca/Sites/LOP/Le islativeSummaries/Bills ls.as•?lan —E&ls=C6&Par1=368cSes=2#P arts%202%20to%205(tx0> under heading "Parts 2 to 5".

enacted its own versions of the provisions set out in the UEEA with respect to the authentication of electronic documents, and the application of the best evidence rule by way of amendments12° to the *Evidence Act*121

The most basic amendment was the inclusion of a functional definition for ESI. Section 34.1(1) of the Evidence Act defines an "electronic record" by mirroring the language in the UEEA as follows:122

> "electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that data, other than a printout referred to in subsection (6); ("document electronique")

Similarly, the *Canada Evidence Act* defines "electronic document" as follows:123

> "electronic document" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

Authentication of Documentary Evidence

All documents need to be authenticated before they can be admitted as evidence. Authentication requires that the documents "must be supported by evidence capable of supporting a finding that the documents are what they purport to be"124 and further "that there is a relationship between the document, an individual, and the issues of the case." This requirement is typically met by "having a sworn witness testify to the identity and source of the document".125 The issue arises "both as a threshold question of admissibility, and again later as a question of weight".126 The authentication issue is most prevalent in cases involving fraud, theft of intellectual property or other criminal-like conduct, or when there has been an acknowledged or proven security breach, or where unauthorized access to a computer or a computer network is known or becomes apparent. With respect to electronic documents, s.31.1 of the *Canada Evidence Act* codifies the conventional common law rule:

---

120 Infra, note12 lat section 34.1 — "Electronic Records".

121 R.S.O. 1990, c. E.23 [Evidence Act].

122 Ibid, at s.34.1(1).

123 Supra notell8 at s.31.8.

124 John D. Gregory, "Authentication Rules and Electronic Records", (2002) 81 Can Bar Rev 529 at p. 557.

125 Ibid. at p.557

126 Eizenga, Michael, "Brave New E-World: The Judiciary at the E-Gate", online: Siskinds LLP <http://www.classaction.ca/pdfipublications/Brave New E-World The Judiciary at the E-Gate.pdf>.

Authentication of electronic documents

31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

Similarly, the Evidence Act of Ontario, in s.34.1(4), imports a similar obligation:

Authentication

(4) The person seeking to introduce an electronic record has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be. 1999, c. 12, Sched. B, s. 7 (2).

A critical aspect of establishing the authenticity of a document, electronic or otherwise, is being able to establish its origin and tracing its subsequent history up to the time of trial — the "chain of custody". In the context of electronic documents, which are readily susceptible to tampering, the chain of custody may be more difficult to establish. In response to this risk, in the context of electronic evidence, "forensic copies, must be created in order to properly preserve the information contained within the electronic file."127 A party seeking to admit into evidence a piece of electronic evidence would be well-advised to carefully document information related to the file's existence prior to its production in the form of a log, which would generally include:128

1. Identification of each piece of evidence;
2. Who had possession , as well as where and when (date, time, location);
3. What was done while the party had possession;
4. What programs and/or procedures were used to copy/move data; and
5. Any change in location.

In light of the ease with which electronic documents may be altered, a party should, at the time of preservation, take care to document information with respect to the device upon which the information was stored, including its make and model number, the extent to which the device was connected to other devices, the date and time recorded on the device at the time of preservation, as

---

127Hrycko, Oleh, Electronic Discovery in Canada: Best Practices and Guidelines, (CCH Canadian Limited: Toronto: 2007) at p.183.

128 Ibid. at p.184.

well as the document's MD5 code.129

Best Evidence Rule

The principle underlying the best-evidence rule is the notion that the administration of justice is best served by insisting that only the best available evidence, often originals, be admissible for judicial consideration. Though its importance has largely been de-emphasized over time, in the modern context, the rule remains applicable to documentary evidence, requiring primary evidence (i.e. an original copy) of any document, where available, that a party adduces for the purposes of relying on its contents, as opposed to establishing its existence.'" Applying the best evidence rule to electronic evidence is difficult given the conceptual difficulty in isolating "original" documents.

In broad terms, the purpose of the UEEA model legislation was to establish a framework that "deals with the admissibility of electronic documents as evidence where the authenticity of the documents and the integrity of the electronic storage system can be demonstrated."131 This is precisely what Parliament set out to accomplish by enacting section 56 of *PIPEDA*, which amended the *Canada Evidence Act* by introducing s.31.2 as follows:

> Application of best evidence **rule — electronic documents**
>
> **31.2** (1) The best evidence rule in respect of an electronic document is satisfied
>
> **a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or**
>
> **b) if an evidentiary presumption established under section 31.4 applies.**
>
> **Subsection 34.1(5) of the** *Evidence Act* **features very similar wording.**

The net effect of these provisions is that, for the purposes of admissibility, as opposed to weight, and the application of the best-evidence rule to electronic documents, the emphasis has shifted away from the document itself onto the underlying system responsible for its

---

129 Ibid. MD5 is an acronym for Message-Digest algorithm 5. By using this cryptographic hash function, a party is able to document a unique identifier akin to a serial number possessed by all digital files. The importance of documenting this information is the fact that where the identifiers associated with two distinct files are the same, there is every reason to believe that the documents are identical and that the original has not been modified. For more information of a technical nature, see http://tools.iett org/html/rfc1321. In the context of satisfying the best evidence rule, Section 34.1(5) of the Evidence Act specifically allows for the proof of the integrity of an electronic records system by adducing evidence that reliable encryption techniques were used to support the integrity of the electronic record.

130 Supra note 97 at p.1217.

131 Damien Mc Cotter & Peter R. Wilcox, "World IP Contacts Handbook", 14th ed., online: Torys LLP < http://www.torys.com/Publications/Documents/Publication%20PDFs/AR2007-19T.pdf > at p.83.

storage. Both the *Canada Evidence Act***I32 and the Ontario** *Evidence Act***133 provide for a statutory presumption which establishes the integrity of an electronic documents system provided the party adducing the evidence can demonstrate that the computer system or device used to store the electronic document was operating properly at all material times. Alternatively, if the system's functioning was compromised, the presumption takes effect so long as it can be demonstrated that the integrity of the record-keeping system was not compromised as a result. A party wishing to rely on either of the legislative presumptions, federal or provincial, also bears the evidentiary burden of establishing that there are "no other reasonable grounds to doubt the integrity of the electronic documents system"134, which in effect means that "a party must be able to establish not only that the system was operating properly on a particular day or over a particular period of time, but that the technology underlying the system was itself capable of producing reliable data to begin with." 135**

In opposing the admission of an electronic document, a party need not disprove the integrity of the electronic documents system but lead evidence to rebut the presumption. Once the presumption is rebutted, it is incumbent on both parties to adduce sufficient evidence in order "[.. 1 to allow the court to decide whether the record-keeping system had sufficient integrity to justify admitting the record."136 This normally takes the form of evidence which speaks to the standards, procedures, usage or practices adopted by a party137. The breadth and degree of sophistication of such evidence will inevitably vary from case to case, and in some circumstances may require the use of an expert witness. In *R. v. Nichols***138, two non-experts, a 9-1-1 operator and the assistant to the Supervisor of the voice recording system of the Peel Regional Police Force, provided the necessary evidence respecting the operation of the electronic document system when the admissibility of a tape recording of a 9-1-1 call was at issue.**

To assist both the private and public sectors, in 2005, the Canadian General Standards Board released a publication139, establishing a national standard providing "policies, procedures, practices and documentation required for establishing the integrity and authenticity of recorded information as an electronic record in an electronic information and records management system."14°

---

132 See Canada Evidence Act s. 31.3.

133 See Evidence Act s. 34.1(7).

134 See Canada Evidence Act, s.31.3(a), Evidence Act s.34.1(7)(a).

135 Supra note126 at p.6.

136 Supra note 110 at p.24.

137 Consistent with the language used in the Evidence Act at s. 34.1(8) and in the Canada Evidence Act at s. 31.6(1).

138 R. v. Nichols (2004), 2004 Carswell Ont 8225 (Ont. Ct. Just) [Nichols].

139 Canadian General Standards Board, "Electronic Records as Documentary Evidence," National Standard of Canada (CAN/CGSB-72.31-2005).

140 Vigi Gurushanta, "CGSB Releases New National Standard on Electronic Records as Documentary Evidence" Calibre Magazine (Volume 11, No.1), online: Canadian General Standards Board <http://www.tpsgc-pwgsc.gc.ca/cgsb/info/news/calibre/011 001/article01-e.html>.

The areas of focus of the policy include:141

data file formats and version control
enabling technologies
quality assurance
metadata capture and preservation
information and records covered by the policy
includes physical and logical structure of info held by the organization
security classification and how to implement it

Implementing and adhering to such a comprehensive standard would assist in establishing admissibility. To establish the integrity of a specific electronic documents system, evidence relating to the following areas should be adduced:142

Sources of data and information — Proof of the sources of the data and the information recorded in the databases upon which the record is based.
This is just another way of saying "garbage in, garbage out";

Contemporaneous recording — Proof that the data and information in those databases was recorded in some fashion contemporaneously with, or within a reasonable time after the events to which such data and information relate. Events and facts have to be recorded soon after they take place;

Routine business data and information — Proof that the data and information upon which the record is based is of a type that is regularly supplied to the computer during the regular activities of the organization from which the record comes. Courts look for data and information that comes from regular business transactions, as distinguished from data and information that is unusual to the business;

Data Entry — Proof that entries into the databases upon which the record is based were made in the usual and ordinary course of business;

Industry Standards — Proof that the input procedures in adding the information to databases conformed to the standard practices in the industry involved. Although national standards for data processing in general do not yet exist, accepted practices within any part of the industry should be conformed to;

Business Reliance — Proof that one has depended on the same information to run the business organization at issue;

Software Reliability — Proof that the computer programs used to produce the printout reliably and accurately process the data and information in the databases involved;

---

141 John D. Gregory, "E-records and the law" (May 14th, 2007) online: <http://www.verney.ca/opsim2007/presentations/301.ppt> at slide 12.

142 Groulx, Karen, "Cookies and Other Electronic Crumbs — The Power of Electronic Discovery", at p.32 citing Ken Chasse, "Chasse 's Cases: The Admissibility of Computer-Produced Business Records is Too Easy", 13 Criminal Lawyers Association Newsletter 1 at p. 29.

A record of records keeping management and control — Proof that records have been kept by a responsible person in charge of the computer and records management system;

Security — Proof of the security features used to guarantee the integrity of the total information or record keeping system upon which the printout is based. This principle has to be the most flexible because security has to vary with the type of information system and use. Such measures could include: (i) protection against unauthorized access to data and to permanent records; (ii) processes for verification of data and statements in records; (iii) safeguarding communication lines; (iv) maintaining copies of records on paper, microfilm, or other reliable physical or electronic form.

The production of a paper print-out of an electronic image (i.e. PDF or TIFF format) of an electronic document containing metadata runs the risk of violating the best evidence rule. In *Armstrong v. Executive Office of the President, Office of Admin*143, the Court acknowledged "[...] that a hard copy paper printout of an electronic document did not include all the information in the computer memory and that it failed to be a complete understanding of what actually happened."144 Further, the Court held that "that paper printouts 'do not affect the record status of the electronic materials unless the paper versions include all significant material contained in the electronic records'"145.

In *ITV Technologies Inc. v. WIC Television Ltd.*-146, a trade-mark infringement case, the plaintiff sought permission to access the internet for the purpose of performing demonstrations at trial, for cross-examining witnesses, and for retrieving electronic versions of documents. The Court adopted the view that "when considering the contents of a web site, the original is found on the Internet and provides better evidence than a print copy.147,, It permitted the parties to access older cached versions of web pages that had since been updated to demonstrate their state of appearance during the relevant time period.

Merely adducing oral evidence with respect to information stored on an electronic device arguably violates the best evidence rule. This was the basis for overturning a criminal conviction in case of *United States v. Bennett*148. In this case, the accused, Mr. Bennett, was charged with illegally importing narcotics into the United States following interception of his boat, believed to be travelling

---

143 1 F.3d 1274, 1283, 1285 (D.C.C. 1993) [Armstrong].

144 AccessData Corporation, White Paper: "The Rules of Digital Evidence and AccessData Technology", online: Access Data <http://www.accessdata.com/downloads/media/Rules of Digital Evidence and AccessData Technology. pdf > at p.4.

145 Jason R. Baron, "E-mail Metadata in a Post Armstrong World", online: National Archives and Records Administration <http://www.archives.gov/era/pdf/baron-email-metadata.pdf> at p.4.

146 ITV Technologies Inc. v. WIC Television Ltd. (2003), 29 C.P.R. (4th) 182 (F.C.T.D.) [ITV Technologies Inc.].

147 Ibid. at para. 13.

148 363 F.3d 947 (9th Cir. 2004) [Bennett].

from Mexico, which was found to contain a large quantity of marijuana. As the boat was intercepted in American waters, the prosecution had to establish that the accused had crossed the border between the United States and Mexico with his payload. At trial, the accused was convicted. On appeal, while his conviction for possession of the narcotics was affirmed, his conviction on the importation charge was overturned on the basis of a violation of the best evidence rule. On the facts of the case, the Customs Officer found a Global Positioning System ("GPS") unit onboard the accused's boat which contained information indicating that the boat had indeed crossed the border. The device was not taken into custody, nor was any of the data on it copied or printed out. According to the United States *Federal Rules of Evidence*, an "original" of data stored in a computer or similar device constitutes "any printout or other output readable by sight, shown to reflect the data accurately"149. In this case, as the officer was merely testifying about the contents of the GPS unit, which amounted to a failure to comply with the best evidence rule, and in the absence of any justifiable explanation for this non-compliance, the officer's testimony was deemed inadmissible, which resulted in the collapse of the prosecution's case.

Hearsay

A classic statement defining hearsay and the presumptive prohibition against its admissibility has been articulated as follows: "[w]ritten or oral statements, or communicative conduct made by persons otherwise than in testimony at the proceeding in which it is offered, are inadmissible, if such statements or conduct are tendered either as proof of their truth or as proof of assertions implicit therein"15° Electronic evidence, as a form of documentary evidence151, falls within this definition. Whether the rule may be invoked turns on the question of the purpose for which evidence is adduced. Thus, "[...] documentary evidence, including e-evidence, may be admitted if it is used to show something other than the truth of its contents or if it falls within an exception to the hearsay rule"152, whether statutory or existing at common law.

The rigidity of a strict category-based approach to the admissibility of hearsay has been softened by the introduction of a principled approach, based on the twin pillars of reliability and necessity. This development in the law did not however do away with the traditional exceptions. Since its introduction153, the principled approach framework has evolved significantly. While the Supreme Court of Canada has subsequently affirmed the primacy of the principled approach to hearsay, parties may continue to resort to the category-based exceptions, under which evidence is presumptively admissible. Nevertheless, evidence sought to be admitted on the basis of category-based exceptions

---

I49See Rule 1001(3), online: Federal Evidence Review <http://federalevidence.com/downloads/rules.ofievidence.pdf>.

150 Supra, note97 at p.229.

151 See R. v. McMullen (1979), 47 C.C.C.(2d) 499 (Ont. C.A.) at 506, R. v. Bell and Bruce (1982), 35 O.R.(2d) 164, 65 C.C.C.(2d) 377 (Ont. C.A.).

152 Supra, note 126 at p.3.

153 While the notion that hearsay evidence may be admissible for the truth of its contents on the basis of its necessity and reliability was first raised in the decision ofAres v. Venner, [1970] S.C.R. 608 (S.C.C.), it was not until R. v. Khan, [1990] 2 S.C.R. 531 (S.C.C.) that the principled approached was formally adopted by the Supreme Court of Canada. See supra, note 97

at p.248. This approach was further developed and refined in R v. Smith, [1992] 2 S.C.R. 915, R. v. Starr [2000] 2 S.C.R. 144 (S.C.C.), and more recently in R. v. Khelawon [2006] 2 S.C.R. 787 (S.C.C.).

is not immune from scrutiny and indeed may be challenged on the basis of failing to meet the standards of reliability and necessity. This was affirmed in R. v. Starr154, which established the following framework for dealing with the admissibility of hearsay evidence:155

a) Hearsay evidence is presumptively inadmissible unless it falls under an exception to the hearsay rule. The traditional exceptions to the hearsay rule remain presumptively in place.

b) A hearsay exception can be challenged to determine whether it is supported by indicia of necessity and reliability, required by the principled approach. The exception can be modified as necessary to bring it into compliance.

c) In "rare cases", evidence falling within an existing exception may be excluded because the indicia of necessity and reliability are lacking in the particular circumstances of the case.

d) If hearsay evidence does not fall under a hearsay exception, it may still be admitted if indicia of reliability and necessity are established on a voir dire.

Business Records Rule

When dealing with documentary evidence, electronic or otherwise, two avenues can be pursued to adduce evidence for the purpose of establishing the truth of its contents. Resort can be made to the common law or statutory exceptions that exist with respect to business records, or, where applicable, under the statutory exception for financial records156. Alternatively, for documents that fall outside the ambit of these rules, one may resort to the principled approach as established in *R. v. Starr* and refined in subsequent jurisprudence.

With respect to business records, the first exception exists at common law and allows for the admissibility of "statements made by a person under a duty to another person to do an act and record it in the ordinary practice of the declarant's business or calling [...] provided they were made contemporaneously with the facts stated and without motive or interest to misrepresent the facts"157 This approach mitigated against the historical concerns surrounding hearsay evidence by relying on "circumstantial guarantees of reliability" 158. The leading authority in this regard is *Ares v. Venner*159.

---

154 [2000] 2 S.C.R. 144 (S.C.C.) [R. v. Starr].

155 As restated in R. v. Mapara, [2005] 1 S.C.R. 358 (S.C.C.) at para. 15, and subsequently cited in R. v. Khelawon, supra note153, at para. 42.

156 See Evidence Act, s.33(2), Canada Evidence Act, s. 29(1).

156 See Evidence Act, s.33(2), Canada Evidence Act, s. 29(1).

157 Supra, note 97 at p.283.

158 Chasse, Ken, "Electronic Evidence: Computer Produced Records in Court Proceedings" , online: Uniform Law Conference of Canada <http://www.ulcc.ca/en/poam2/index.cfm?sec=1994&sub=1994ac > at para. 31.

159 [1970] S.C.R. 608 (S.C.C.) [Ares].

Nevertheless, as a consequence of subsequent legislative provisions enacted both federally and provincially, which expressly permit the admission into evidence of business records, this common law doctrine is of limited relevance in all but two provinces across Canada.166 In those provinces, or in other limited circumstances elsewhere, the *Ares* decision remains relevant. Consequently, although the business records exception remains relevant, admission of such records is primarily statute based.

These legislative provisions161 have effectively carved out an exception to the hearsay prohibition for documents generated in the course of carrying on business provided certain conditions are met. The business records exception does not require that the truth of the actual contents of the record be proven. The fact that a record was created and relied upon in the course of business provides sufficient proof to support the admission of the record."

There are two basic requirements under most provincial statutes:

1. The record must have been made in the usual and ordinary course of business;
2. It was in the usual and ordinary course of business to make that record.

If it is in the usual and ordinary course of business to make a record, but not to enter the record into a computer system, then the computer record may not satisfy the second part of the test. While the wording of the federal and provincial provisions is similar, there are some important differences between them that should be noted. For example, the definition of "business" in Ontario does not extend to government, whereas the federal statute specifically contemplates government activity. Moreover, unlike the federal statute, "half of the provincial statutes impose a further requirement that 'it was in the usual and ordinary course of business to make the writing or record at the time of the act, transaction, occurrence or event, or within a reasonable time thereafter'"162, which imposes an additional admissibility requirement, namely that the employee was under a duty to create it. This is illustrated in the decision of *R. v. Laverty*.163 Lastly, whereas the Federal statute expressly excludes documents made in certain circumstances164 in Ontario "the circumstances of the making of any writing or record may affect its weight but not its admissibility."165

Protective Orders

Protective orders are the product of a process to balance the competing values of an open and accessible court proceeding against serious risks of harm to commercial interests. The seminal

---

160 Alberta and Newfoundland and Labrador do not currently have a provincially legislated framework with respect to the admissibility of business records.

161 See Evidence Act, s.35(2); Canada Evidence Act, s. 30(1).

162 Supra note 109 at p.103.

163 Ibid., citing R. v. Laverty (1979), 9 C.R. (3d) 288 (Ont. C.A.).

164 See Canada Evidence Act, s. 30(10).

165 Supra note 109 at p.101, see Evidence Act s.35(4).

decision in this area of the law is *Sierra Club of Canada v. Canada* (*Minister of Finance*)166, a case involving the judicial review of proceedings initiated by an environmental organization, Sierra Club ("Sierra Club"), against a Crown Corporation, Atomic Energy of Canada Ltd. ("Atomic Energy"), involved in the construction and sale of nuclear reactors to China. Sierra Club sought to overturn the federal government's decision to provide financial assistance to Atomic Energy. At the heart of this decision were confidential environmental assessment reports originating in China, which Atomic Energy sought to protect by way of a confidentiality order. Atomic Energy's application before the Federal Court, Trial Division167 was rejected, and the appeal from this decision was dismissed by all but one judge of the Federal Court of Appea1.168 On further appeal to the Supreme Court of Canada, Atomic Energy was ultimately successful in obtaining the relief it was seeking. In arriving at its conclusion, a unanimous Supreme Court reasoned:169

> A confidentiality order should only be granted when (1) such an order is necessary to prevent a serious risk to an important interest, including a commercial interest, in the context of litigation because reasonably alternative measures will not prevent the risk; and (2) the salutary effects of the confidentiality order, including the effects on the right of civil litigants to a fair trial, outweigh its deleterious effects, including the effects on the right to free expression, which in this context includes the public interest in open and accessible court proceedings. Three important elements are subsumed under the first branch of the test. First, the risk must be real and substantial, well grounded in evidence, posing a serious threat to the commercial interest in question. Second, the important commercial interest must be one which can be expressed in terms of a public interest in confidentiality, where there is a general principle at stake. Finally, the judge is required to consider not only whether reasonable alternatives are available to such an order but also to restrict the order as much as is reasonably possible while preserving the commercial interest in question.

In this case, the commercial interests at stake, namely the preservation of contractual confidentiality obligations, was sufficiently important to meet the first prong of the test, and there were no reasonable alternatives to granting the order. Not granting the order would adversely affect Atomic Energy's right to a fair trial, as it would force the organization to withhold the confidential documents, which would affect its ability to mount a defence, and further impede in the truth-seeking process of trial. Any deleterious effects that the order might have had on the freedom of expression were mitigated by the narrow scope and highly technical nature of the information in question.

---

166 Sierra Club of Canada v. Canada (Minister of Finance) (2002), 211 D.L.R. (4th) 193 (S.C.C.) [Sierra Club].

167 Sierra Club of Canada v. Canada (Minister of Finance) (1999),1999 CarswellNat 2187 (F.C.T.D.).

168 Sierra Club of Canada v. Canada (Minister of Finance) (2000), 2000 CarswellNat 3271 (F.C.A.).

169 See head note, supra note166

Cost Issues

As a general proposition, while "the interim costs of preservation, retrieval, review and production of electronic documents will be borne by the party producing them"170, the cost associated with the reproduction of these documents is to be borne by the party requesting them.171 As a consequence, in the context of electronic discovery, a party may be faced with extraordinary costs and disbursements in meeting its disclosure obligations, which may in effect prevent it from having its case decided on the merits. Moreover, the cost implications associated with carrying out one's discovery obligations in the e-discovery context can be determinative because it forces a party to choose settlement over reviewing what is effectively truckloads of data. While it is generally the case that a portion of the costs associated with these efforts may only be recouped by the successful party at the end of the litigation172, the court has the discretion to make interim costs orders. 173 Where accessing the data may require extraordinary effort and cost, because of the media on which the data is stored, "[...] it is generally appropriate that the party requesting such extraordinary efforts should bear, at least on an interim basis, all or part of the costs of doing so."174

The recent amendments to the Ontario *Rules of Civil Procedure*175 introducing the concept of proportionality to the discovery process recognize the unique problem presented by ESI. The sheer volume of data, the number of locations where electronic data may be stored, the relative permanence of this data, and the costs and burden that may be imposed on the party subject to the preservation obligation, requires preservation measures to be proportionate. Several recent cases have dealt with this issue, where courts have denied broad production requests and instead substituted narrower and more specific orders for production that place a smaller burden on the parties176. For example, in Borst v. Zilli177 Master Brott considered the proportionality principle in granting a costs shifting order. The parties had reached an agreement to retain an independent computer consultant ("ICC") who would obtain a copy of the computer data and an independent solicitor ("ISS") who would review the documentation for relevancy and privilege. The parties disagreed about who should pay for the ICC and the ISS. The defendants contended that because the plaintiffs sought the information they should pay. Master Brott stated:

---

170 Supra note 30 at p.17.

171 See sub-rule 30.04(7) of the Rules of Civil Procedure, supra note 9.

172 See Re Regional Municipality of Hamilton-Wentworth and Hamilton-Wentworth Save the Valley Committee, Inc. (1985), 51 O.R. (2d) 23 (Ont. Sup. Ct. — Div. Ct.), at p. 32. But also see British Columbia (Minister of Forests) v. Okanagan Indian Band, [2003] 3 S.C.R. 371 (S.C.C.), a case in which the Court held that as an exception to the general rule, interim cost awards should only be made where certain conditions are met.

173 Groulx, Karen, "The Issue of Costs", LawPRO Magazine, September 2005, Vol.4, Issue 2, at p.9. See s.131(1) of the Courts ofJustice Act, R.S.O. 1990, c. C.43 which operates in conjunction with Rule 57.01(1) of the Rules of Civil Procedure, supra note 9, which lists factors that a court may consider when awarding costs.

174 See supra note 34 at p.39, under the commentary relating to Principle 12.

175 Supra, note 30.

176 See Vector Transportation Services Inc. v. Traffic Tech Inc. (2008), 58 C.P.C. (6th) 364; [2008] O.J. No. 1020 (Ont. Sup. Ct.) and Matheson v. Scotia Capital Inc., [2008] O.J. No. 3500 (Ont. Sup. Ct.).

177 [am] O.J. No. 4115 (Ont. Sup. Ct.).

> "The Sedona Canada principles recognize that when considering disclosure requests and standards for disclosure the courts must balance a number of factors. The courts apply the principle of proportionality to ensure that the costs of discovery do not unduly interfere with a just, speedy and inexpensive resolution of a dispute."

Existing jurisprudence on the issue of cost-shifting with respect to electronic documents in the Canadian context is scarce. It should be noted that although there is a wealth of American jurisprudence on this issue, given fundamental differences between the United States and the common law jurisdictions in Canada with respect to how the issue of costs is resolved, its relevance in the Canadian context is limited.178 In *Bank of Montreal v. 3D Properties*-179, the defendant applied to the Court for an order compelling the plaintiff financial institution to produce various documents including computer records, discs and tapes. Though the Court would allow the defendant's request, it saw fit to impose all reasonable costs associated with searching for, locating, editing and producing the sought-after documents on the applicant, leaving what constituted "reasonable costs" to be determined as between the parties, or by the Court upon further application should they be unable to reach a consensus. By contrast, in Cholakis, the Court ordered that the defendants would bear the costs of reviewing and modifying its software in order to limit its production of data in accordance with an earlier court order. It further held that the expense involved in carrying out this task "may be a disbursement to be considered in an Order for costs at a further stage in the proceedings."18°

In *,IDS Uniphase Inc. v. Metconnex Canada Inc.*181 , both parties agreed, by way of written agreement, to exchange and produce their respective documents in a common format, namely a "summation" database, and retained the same service provider to accomplish this task. After receiving the plaintiff's materials, the defendant concluded that they had serious deficiencies. After some negotiation, the parties agreed that the plaintiff would produce a database with the same functionality as that of the defendant, which involved an additional cost, one half of which the defendant agreed to pay. The defendant ultimately sought to have its one-half contribution to this cost reimbursed. The Court refused to grant this relief, concluding that the dispute might have been caused by a lack of familiarity with e-discovery rather than any intent to shirk discovery obligations. Given the plaintiff's offer to bear half of the additional cost to bring its database up to the higher standard, the Court was unprepared to grant the relief sought absent "additional information with respect to the long-term benefits of producing the electronic database in the enhanced format."1" Alternatively, the Court required evidence that "the costs of the electronic production resulted in a disproportionate burden for

---

178 The United States does not follow the same "loser pays" model to costs apportionment that is prominent in Canadian common law jurisdictions. See Glenn A. Smith, "E-discovery: Can the Clients Afford It?" online: SLAW <http://www. slaw. ca/200 9/0 1/10/e-discovery-can-the-clients-afford-it>.

179 Bank ofMontreal v. 3D Properties (1993), 1993 CarswellSask 159 (Sask. Q.B.) [Bank ofillontrea].

180 Ibid. at para.35.

181JDS Uniphase Inc. v. Metconnex Canada Inc. (2006), 2006 CarswellOnt 6264 (Ont. S.C.J.) [JD Uniphase Inc].

182 Ibidc at para. 12.

one of the parties"183, which was not the case here as the Court noted that both parties were able to pay for the costs of litigation.

In *Barker v. Barker*-184, the Plaintiffs commenced an action against the Province of Ontario and two individual doctors with respect to treatment they received at a provincial mental health centre. In an effort to satisfy their disclosure obligations, the defendants proposed digitizing documents consisting of the medical and personal records of the plaintiffs in the possession of the Crown. These amounted to between 50,000 and 100,000 documents, and converting them to a digital format would cost between $160,000 and $383,000. The defendants sought an order requiring the plaintiffs to fund one third of the cost of conversion. The plaintiffs objected to this request primarily on the basis that they were impecunious and that such an award would force them to abandon their claim. The Court ultimately ordered that the plaintiffs pay one-third of the costs of conversion, on a provisional basis. It noted that: "the benefits for the litigation process from electronic storage, coding and other retrieval facilities are likely to be far more significant in cases like this where productions are old, fragile and voluminous"1" and further that there were "very substantial continuing benefits to the plaintiffs and the court that are likely to be obtained from the conversion of the defendants' productions into electronic form" 186 beyond the discovery phase.

Conclusion

Businesses not only depend on computers to record their business activities but are now required to produce those records (to the extent they are relevant) in electronic form. Parties seeking to avoid the sting of their electronic words or deeds often seek to discredit the electronic evidence being relied upon by their opponents principally by attacking the authenticity of the evidence. Good record keeping practices coupled with the help of computer forensic experts can help to refute these objections to the use of electronic evidence.

---

183 Ibid.

184 Barker v. Barker (2007), 2007 CarswellOnt 2448 (Ont. S.C.J.) [Barker].

185 Ibid at para. 14.

186 Ibid at para. 15.

Dentons Canada LLP

T +1 416 361 2381
F +1 416 863 4592
dentons.com