Lex Electronica
Revue du Centre de recherche en droit public

Email Evidence Preservation

How to Balance the Obligation and the High Cost

Jie ZHENG

Lex Electronica, vol. 14 n°2 (Automne / Fall 2009)

I. Introduction

Computer technology has revolutionized the way we deal with information and the way we run our business. Increasingly, important business information is being created, stored and communicated electronically. It is estimated that 97 percent of business documents are created electronically and more than 35 percent never reach paper.[1] Such electronic data is now being routinely requested during the course of litigation. E-mail, as a distinctive type of electronic evidence, becomes more and more important in electronic discovery.

In order to fulfill the legal obligation to produce e-mail evidence by the requesting party and reduce the risk of losing the case by failure to provide evidence, companies are advised to preserve the relevant e-mail evidence. However, considering the expensive storage administration fee, companies also undertake a heavy burden of preserving the great volume of e-mails that they generate.

This paper discusses the practical dilemma between the obligation of e-mail evidence preservation and the high cost of the preservation and then makes suggestions on how to strike the balance between the two from the perspective of the parties and the court.

II. E-mail in Electronic Evidence

A. Definition and Characteristic of E-mail Evidence

1. Definition

Electronic evidence refers to electronic data which is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal case. Electronic mail is the telecommunication of messages from one computer to another.[2] It is one of the electronic evidence that is widely used in electronic discovery nowadays.

Due to the heavy dependence of many businesses on electronic communications, as much as 80 percent of discoverable communications will be in the form of e-mail because it is often the primary tool for business and personal communications.[3]

[1] G Coumbe, "E-Discovery" (2004) The New Zealand Law Journal at 130.
[2] Benjamin Wright: *The Law of Electronic Commerce EDI, Fax, and E-mail: Technology, Proof, and Liability* (Boston: Little, Brown & Co., 2nd ed., 1995) at 6.
[3] Paul R. Rice: *Electronic Evidence Law and Practice* (Chicago: American Bar Associations 2005) at 3.

2. Characteristics of E-mail evidence

E-mail evidence in most cases provides most damaging information because people commonly perceive e-mails as similar to a telephone conversation and often use emails as an informal means of communication.

(1) E-mail is informally edited.

E-mail is a hybrid form of communication. It provides the users the opportunity to communicate casually, as they would in a typical conversation, even though a permanent record may be created. People frequently take less care in composing e-mails than they do when writing formal letters or memoranda, which create potential problems in litigation.

(2) E-mail is hard to delete.

Unlike paper records, it is difficult to delete all traces of e-mails and the e-mails can still be discoverable. People tend to think that the information has been deleted completely by clicking the delete key. However, deleting only means that the computer finds the data's entry in the disk directory and changes it to a "not use" status.[4] Even deleted e-mails can be recovered by forensics experts. Since e-mails tend to be stored in more locations and typically distributed to a wider audience than paper documents, the task of finding and erasing all copies and traces of a document can be much more challenging.

(3) E-mail is easily forged.

E-mail is more susceptible to after-the-fact-alteration. It is fragile and may be intentionally or unintentionally modified by turning on a computer which can overwrite existing files.[5] Most e-mail systems, allow people to edit the message before forwarding it. Such alteration wouldn't be discernible to the recipient. However, the integrity of the evidence requires that no one is able to modify the e-mail before it is reached to the receiver. Also, e-mail is sometimes written without signature of the sender, which arise problems in the identification of the sender.

B. The comparison and contrast between E-mail evidence and paper evidence

Evidence is anything that demonstrates, clarifies, or shows the truth of fact or point in question.[6] Paper has been a reliable medium to hold legal evidence for centuries. Electronic messages seek to eliminate the exchange of paper between trading partners and minimize the paper records each retain. It has become a more and more important way of evidence that has been accepted by the courts in litigation. Courts are taking a keen interest in this new area and are working through the application of existing rules and statutes to meet this technological reality.

---

[4] X-tech Group: "Email as evidence, 'Smoking Guns' Hiding in your Inbox" (2004) online:
< http://www.simpsongrierson.com/assets/expertise/xtech/publications/it/2004/KYN_June04.pdf >.

[5] Cecilia K.Garrett, "Admissibility of Electronic Information" (2002) 71-SEP.J.Kan.B.A.33 at 33.

[6] *Supra* note 2 at 98.

1. Similarities between e-mail evidence and paper evidence

(1) In Written Form

Evidence is required to be original and authentic. Most jurisdictions have accepted that electronic data stored inside a computer system may constitute a "document" and that the rules of documentary evidence govern its admissibility.[7] Although e-mail evidence is kept in the computer, during the discovery period, in order to be admitted as effective evidence, e-mail evidence should also be provided in written form, so as the paper document.

(2)The Objective of Evidence

As communication records, e-mail evidence and paper evidence both aim to prove some fact of consequence. Thus, they all bear the objective of showing the logical connection between the evidence and the legal fact that it is offered to prove.

(3) Legal Effect in Litigation

Within the wide use of e-mail in commercial transactions, e-mail evidence is deemed as equivalent of paper-based documents in litigation. At the same time, e-mail evidence is also subject to the same rules and laws that apply to documentary evidence.

2. Differences between e-mail evidence and paper evidence

(1) Destructibility

Compared to paper evidence, e-mail evidence is much more difficult to destroy. Once the paper evidence is being disposed through various ways, the document is gone and is not likely to be resurrected. In contrast, the e-mail evidence is not so easily destroyed. It tends to remain accessible on a computer hard drive even after it has been "deleted". In *Prism Hospital Software Inc. v. The Hospital Records Institute*[8], the defendants produced a quantity of magnetic media from which the plaintiff was able to locate a series of files that, though "deleted", continued to exist.

(2) Storing volume

The storage volume of paper requires significant physical space. To keep the paper documents retrievable, the companies have to keep piles of paper documents in stock for a certain period of time and ultimately destroy them. In contrast, computer storage takes very little physical space and is relatively inexpensive. Unlike paper documents, e-mails are not necessarily stored in any organized rationale, significantly complicating its review and production.

[7] Alan M.Gahtan: *Electronic Evidence* (Ontario: Carswell Legal Pubns 1999) at 138.
[8] *Prism Hospital Software Inc. v. The Hospital Records Institute* (1991), 62 B.C.L.R. (2d) 393 (S.C.).

(3) Attitude

People tend to believe that there is something transient, impermanent and casual about electronic communication.[9] Thus, electronic communication may contain more unguarded spontaneous remarks than any other previous form of human communication. People often write e-mails casually and little care is given to grammar and context. Their signature or even their name may be omitted.[10] E-mails are more carelessly written than the paper document, which may be used as evidence in discovery.

(4) Requirements

Generally speaking, evidence is required to be relevant and authentic. Unlike paper with the original version and the copy version, e-mail evidence does not enjoy the same presumption of authenticity. E-mail evidence is easily changed by adding or deleting content, making changes to file attributes or modifying the metadata that records information. To be admissible in court, e-mail evidence must be relevant, material, integral and authentic.

C. Admissibility and authentication of e-mail evidence

1. Authentication of e-mail evidence

To be admitted as evidence, an electronic message must first be authenticated or identified. Authentication is the process by which the authenticity, or genuineness, of a document is established.[11] Whether a document is what it purports to be is a matter of conditional relevance i.e. the document is relevant only if the document is what it purports to be.[12]

E-mails are composed of a "header" and "body". While the body of the e-mails contains the individual text composed by the sender, the header listing the sender's name and address, the recipient's user name and address, the transmission date and time and the subject matter of the mailing. If email is produced by a party from the party's files and on its face purports to have been sent by that party, these circumstances alone may suffice to establish authenticity.[13] Authentication should be made through a knowledgeable witness who can identify the authorship as well as the document's appearance, contents, substance, internal patterns, or other distinctive

[9] Michele C.S. Lange & Kristin M. Nimsger: *Electronic Evidence and Discovery: What Every Layer Should Know* (Chicago: ABA 2004) at 7.

[10] Beatrice O'Donnell & Thomas A. Lincoln , "Authenticating E-mail Discovery as Evidence" The Legal Intelligencer (13 August 2007) online:
Law.com <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1186736525985 >.

[11] *Supra* note 7 at 157.

[12] Mark D. Robins, "Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation" (2003) 29 Rutgers Computer & Tech. L.J. 219 at 225.

[13] Gregory P. Joseph, "Trial Evidence in the Federal Courts: Problems and Solutions Sponsored with the Cooperation of the ABA Section of Litigation: Internet and Email Evidence"(2008) American Law Institute 559 at 579.

characteristics.[14] Given that most e-mails contain certain identifying markers, such as the address from which they were sent, the name of the sender, or a company name, that information, coupled with their production during discovery, should be enough to satisfy the authentication requirements.[15]

However, new technology requires new rules of authentication of e-mails, which lead to the uncertainties of authenticity for e-mail evidence on a case-by-case basis.

2. Admissibility of e-mail evidence

Electronic evidence, as a type of "documentary evidence" must satisfy the same rules as are required for traditional documentary evidence to be admitted into evidence. It is subject to civil discovery in the same manner as paper documents.

The best evidence rule requires that a party adduce the best evidence available, which in respect of documentary evidence, means that the original of a writing be offered into evidence.[16] When introducing this rule to electronic evidence, it is required that whether a computer printout is an "original" or a "copy". The requirement of originality for paper document is applied differently in e-mail evidence. If data are stored in a computer or similar devise, any printout readable by sight, shown to reflect the data accurately, is deemed as "original".[17]

The *Canada Evidence Act* uses the rule that measures the admissibility of the secondary evidence, or copies, against the "original document", rather than just a "record made in the usual and ordinary course of business". The Ontario Court of Appeal in *R. v. Bell*[18] held that computer printouts were not merely "copies", but were in fact "original records".

To admit e-mails into evidence, the proponent must show the origin and integrity of e-mails. He must show who or what originated the e-mail and whether the content is complete in the form intended, free from error or fabrication. In discovery, the proponent needs to prove that the hard copy of the e-mail evidence is consistent with the one in the computer and includes all the information held in the electronic document.[19]

---

[14] Hon, William J. Haddad, "Authentication and Identification of E-mail Evidence" (2008) 96 ILBJ 252 at 254.
[15] Thomas J. Casamassima & Edmund V. Caplicki III, "Electronic Evidence at Trial: The admissibility of Project Records, E-mail, and Internet Websites" (2003) 23-SUM CONSLAW 13 at 17.
[16] *Supra* note 7 at 151.
[17] *Supra* note 3 at 194.
[18] (1982), 35 O.R. (2d) 164 (Ont. C.A.), affirmed (sub nom. *Bruce v. R.*) [1985] 2 S.C.R. 287 (S.C.C.).
[19] Leah Voigt Romano, "Developments in the Law: Electronic Discovery: VI. Electronic Evidence and the Federal Rules" (2005) 38 Loy.L.A.L.Rev.1745 at 1796.

III. Requirements of E-mail evidence preservation

The common law duty to preserve evidence extends to electronic discovery. If a party is unable to produce the requested evidence, the Court may allow jurors to presume that the lost evidence would have supported the other side's claim. The preservation obligation necessarily involves two related questions: when does the duty to preserve attach, and what evidence must be preserved. [20]

A simple answer to the first question is that, same as in traditional discovery, the commencement of litigation triggers the preservation obligation in electronic discovery. The second inquiry about the scope of preservation obligation is more complicated. As a general rule, the producing party should make reasonable efforts to identify and manage the relevant information readily available.

A. Case Law

In many courts, it is a fairly routine matter to get computer-generated documents admitted into evidence. E-mail evidence has occurred frequently in employment disputes and antitrust cases.

1. The legal liability of E-mail evidence spoliation

Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence, in pending or future litigation."[21] The concept of sanctioning for spoliation originated in the common law doctrine "*contra spoliatorem omnia praesumuntur*", which means "all things are presumed against destroyer".[22] Therefore, the principal of spoliation should also be applied in electronic evidence. With increasing frequency, litigants are raising spoliation charges alleging the failure of their opponents to adequately preserve electronic evidence. Courts will need to strike a balance between the need to preserve relevant evidence and the reality that not all potentially relevant electronic material can be preserved at all.

(1) Employment disputes

In *Zubulake v. UBS Warburg LLC*[23], a securities trader, Laura Zubulake, charged UBS Warburg (her former employer), with gender discrimination and retaliation. Zubulake requested, in discovery, the production of all communications, including e-mails, relating to her that were sent or received by five specified employees over a two and one-half year period. A $29 million verdict was returned against UBS because the company had destroyed email messages that were demanded as evidence in the case. In ruling upon Zubulake's request to sanction UBS, the court

[20] William J. Robinson, " An Overview of Electronic Discovery" (2005) Practicing Law Institute 189 at 194.
[21] Willard v. Caterpillar, Inc., 40 Cal. App 4th 892, 907, 48 Cal. Rptr.2d 607,616 (1995).
[22] *Supra* note 3 at 48.
[23] Zubulake v. UBS Warburg LLC, 216 F.D.R. 280 (S.D.N.Y. 2003)

explained that a business must impose a "litigation hold" on routine data destruction in certain circumstances. This "duty to preserve" records arises at a minimum when a business receives notice that a formal administrative or judicial proceeding has been filed and, ever sooner, if the business has reason to believe that litigation is on the horizon. However, parties don't need to preserve every shred of paper, every email or electronic document, and every backup tape, nor does preservation obligation require freezing of all electronic documents and data, including e-mail.

> "*Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation. As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation.*"[24]

(2) Heritage Dispute

In *Tarling v. Tarling*[25]**,** the Ontario Superior Court of justice has considered a tort claim for spoliation since the Ontario Court of Appeal held, in Spasic Estate, that a claim based on the tort of spoliation should not be struck out for failing to disclose a reasonable cause of action.

One son is alleging that the other influenced the father to alter his will in his favor. The plaintiff established that the defendant arranged to have the testator's computer wiped after the plaintiff threatened litigation and after he had received correspondence from the plaintiff's counsel. The plaintiff also established that there was at least one e-mail destroyed (which was later produced from a third-party) which supported his claim that the defendant asserted undue influence over the testator. He argues that this is a basis for a substantive claim for damages as well as a reason for the court to impose sanctions.

In very brief treatment the Court seems to accept that a claim for tort damages for spoliation can be made out on mere proof of bad faith destruction of evidence. However, in rejecting the claim it implied that prejudice is also a requirement. The court concluded

> "*In my opinion, this e-mail is no more unfavourable to William Jr. than other e-mails that he did produce that show his involvement in William Sr.'s dispute with Frank. In light of this and in view of the significant volume of documents that William Sr. did produce, I am unable to conclude that William Jr. intentionally destroyed relevant evidence. In the result, Frank's claim for damages arising from William Jr.'s destruction of documents is dismissed. Similarly, I cannot, in the circumstances, conclude that any other sanction for the destruction of documents is warranted."*

The Court did not consider whether the defendant had a positive duty to take reasonable steps to preserve the testator's computer or the nature and extent of such a duty.

---

[24] *Ibid.*

[25] Tarling v. Tarling, 2008 CanLII 38264 (ON S.C.)

2. E-mail evidence in anti-trust dispute

In the well-known *United States of America v Microsoft Corporation*[26], the government collected in discovery more than 3 million documents, many of which are e-mails, to use against Microsoft. These e-mails became important evidence to help support the government's argument of anticompetitive behavior and the lack of credibility of Microsoft's evidence. The messages extracted from the company's computers during a four-year investigation, has been used by the government to argue that many of Microsoft's key business decisions -- including the integration of Internet browsing technology in its flagship Windows software -- violate antitrust laws.

Same case happened on Intel Company in anti-trust dispute. Advanced Micro Devices Inc (AMD) filed antitrust charges against Intel on June 27 2005.[27] It claims Intel has used illegal payments or improper subsidies to strong-arm a range of computer makers, distributors, and retailers into not selling or supporting AMD microprocessors. The Intel acknowledged the loss of potential e-mail evidence due to human error and most of the missing e-mails were written after AMD filed suit against Intel according to court document. The judge ordered Intel to try to recover the lost e-mails that was required to an anti-trust lawsuit filed by AMD. With countless documents and hundreds of witnesses to sort through, chip maker Advanced Micro Devices' antitrust lawsuit against Intel won't begin until 2010 at the earliest. However, it is obvious that Intel will undertake the legal liability if it cannot provide e-mail evidence and fails to meet its burden of proof.

B. Legislation in Canada

1. Federal legislation: *Canada Evidence Act*

"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.[28] 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.[29]

---

[26] (2007) 87 F Supp 2d 30; United States of America v Microsoft Corporation 253 F.3d (DC Cir 2001).
[27] Chris Preimesberger, "Intel Faces Up to E-mail Retention Problems in AMD Lawsuit" (7 March 2007), online: < http://www.eweek.com/c/a/Data-Storage/Intel-Faces-Up-to-EMail-Retention-Problems-in-AMD-Lawsuit/ >.
[28] *Canada Evidence Act*, R.S.C. 1985, c. C-5, Art.31.1.
[29] *Ibid* Ar. 31.8.

2. Provincial legislation

(1) *Civil Code of Quebec*

In the *Civil Code of Quebec*, proof of a fact or juridical act may be made by a writing[30], which is a means of proof whatever the medium, unless the use of a specific medium or technology is required by law. Where a writing is in a medium that is based on information technology, the writing is referred to as a technology-based document within the meaning of the Act to establish a legal framework for information technology.[31]

(2) An Act to Establish a Legal Framework for Information Technology

A technology-based document may fulfill the functions of an original. To that end, the integrity of the document must be ensured and, where the desired function is to establish[32]:

1) that the document is the source document from which copies are made, the components of the source document must be retained so that they may subsequently be used as a reference;

2) that the document is unique, its components or its medium must be structured by a process that makes it possible to verify that the document is unique, in particular through the inclusion of an exclusive or distinctive component or the exclusion of any form of reproduction;

3) that the document is the first form of a document linked to a person, its components or its medium must be structured by a process that makes it possible to verify that the document is unique, to identify the person with whom the document is linked and to maintain the link throughout the life cycle of the document.

C. Practical Dilemmas: strike a balance between the obligation to preserve the relevant e-mail evidence and the high cost of e-mail evidence preservation.

1. The obligation to preserve the relevant e-mail evidence

E-mail, when printed in hard copy or stored electronically, is usually recognized as equivalent to a paper document. Parties should take reasonable and good faith steps to meet their obligations to preserve information relevant to the issues in an action.[33] Under the spoliation of evidence doctrine, when evidence is spoiled, destroyed, or is simply not retained, the party may be entitled to a jury instruction or judgment unfavorable to the adverse party based on the presumption that the evidence was not preserved. The producing party is responsible for retrieving relevant record and information demanded by the discovering party. The parties involved in the legal dispute must know what kind of evidence should be preserved when there is potential relevance in the litigation. However, the scope of what is to be preserved and the steps

---

[30] Art. 2811 C.C.Q.

[31] Art. 2837 C.C.Q.

[32] *Legal framework for information technology, An Act to establish a,* R.S.Q. c. C-1.1, Art.9.

[33] *Sedona Canada Principles* at 13, online: <http://www.lexum.umontreal.ca/e-discovery/The%20Sedona%20Canada%20Principles%20-%20Handout%20Version%202008.pdf >.

considered reasonable may vary widely depending upon the nature of the claims and information at issue.

The inability to produce the material of one party can hinder the legal process and damage the party's chance of prevailing in the case, or even make the party subject to fines and other punishment by the court.[34] If one party fails to provide e-mail evidence requested by the other party, it is more likely that the party will take the risk of losing the case and undertake the indemnity. Thus, it is obligatory for the parties to preserve the relevant e-mails in order not to be in a disadvantaged position in the litigation.

2. The high cost of preservation management

Although the price of disk space is getting cheaper, the storage administration is getting more and more expensive. It includes the cost of retrieving the important e-mails and producing the material, client costs as well as counsel fees. The costs of discovery are traditionally borne by the producing party. Any other cost-shifting generally occurs at the end of the litigation, at which time the unsuccessful party may be required to contribute, in whole or in part, towards the costs of the successful party.

Large companies bear disproportionate risks and burdens, in part because of the greater volume of e-mails they generate. Burdensome e-mail discovery requests most frequently are propounded in securities fraud, tort and employment cases where individuals sue large entities.[35] Under these circumstances, different considerations should be given when the large entities make extraordinary effort to provide a large amount of evidence. In such cases, requiring the producing party to fund the significant costs associated with restoring such data may be unfair, and may hinder the party's ability to litigate the dispute on its merits. Accordingly, 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.

3. How to strike the balance?

(1) ***Parties:*** Adoption of "Data Retention and Destruction Policy"

The existence of a document management policy may, under certain circumstances, be deemed a mitigating factor in litigation even when documents are destroyed pursuant to it. On

[34] Deb Shinder, "Authentication, Access Control & Encryption: Documenting Authenticity of Evidence for the E-discovery Process" (16 July 2008) online: Windows Security <http://www.windowsecurity.com/articles/Documenting-Authenticity-Evidence-E-Discovery-Process.html >.

[35] Ian C. Ballon, "Spoliation of E-mail Evidence: Proposed Intranet Policies and a Framework for Analysis" Cyperspace Lawyer (March 1999) online: Findlaw < http://library.findlaw.com/1999/Feb/22/131004.html >.

the other hand, a company's failure to have a coherent policy may be an aggravating factor.[36] Thus, it is necessary for the litigants to have a data retention and destruction policy. Such a policy, when utilized prior to any litigation, can help protect a company from sanctions when documents are not retained.[37] In order to keep the document retention policy neutral, the litigants should also periodically revise the policy when new case law or statutes impose additional record retention requirements.

A proper policy should include: (1) an inventory of electronic devices and data storage, with reference to backups and archives; (2) a specific schedule detailing when which types of documents will be destroyed and when backups or archives are to be erased; (3) a records custodian who manages and enforces the policy; (4) employee training with regard to the policy's impact on day-to-day business operations; and (5) an easily accessible copy of the policy and any related guidelines.[38]

Taking into consideration the cost of document management before the case, the cost of collecting e-mail evidence in the case and the cost of indemnification after the case, not having electronic data easily accessible can be costly in future litigations. Under a well-managed data retention and destruction policy, the litigants can set up a steady and routine data retention period which reduces the high cost of e-mail evidence collection in the late litigation stage.

(2) ***Court:*** E-mail should not be treated exactly the same as a paper document for purpose of discovery.

E-mail is quite different from the formal written documents in that they are casually written and easily forged. It should not be treated exactly the same as a paper document in the requirement of evidence preservation.

The court should first consider the cost of collecting e-mail evidence before deciding to impose the burden of proof on one party. In addition, it should also reduce the burden of litigant with e-mail retention and destruction system.

IV. Conclusion

E-mails are routinely received, stored, copied and deleted by companies on a daily basis. It is one of the most frequently used tools in business litigation. E-mail evidence is a double-edged sword in e-discovery: on the one hand, it can be used as evidence in support of a company's litigation; on the other hand, it can also be used against a company.

A litigant is under no duty to keep or retain every document in its possession once a complaint is filed. It is only under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence,

[36] Compare Willard v. Caterpillar, Inc., 40 Cal, App. 4th 892, 921, 48 Cal. Rptr.2d 607, 625 (1995).
[37] Edward T. Ellis, "Evidentiary Issues In Employment Cases" (2008) The American Law Institute 1023 at 1075.
[38] *Ibid.*

is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and is subject to a pending discovery request.[39]

There is no universal legal guidance on when the preservation obligation arises, the scope of electronic evidence that must be preserved or how to properly balance the costs. With the booming cases of e-mail evidence, more and more jurisprudence will make the rules of e-mail evidence preservation clear and expectable.

[39] William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp.1443, 1455 (C.D. Cal. 1984) & Turner v. Hudson Transit Line, Inc., 142 F.R.D. 68, 73 (S.D.N.Y. 1991).

BIBLIOGRAPHY

LEGISLATION

Canada Evidence Act, R.S.C. 1985, c. C-5.
Civil Code of Quebec (L.Q., 1991, c. 64).
Legal framework for information technology, An Act to establish a, R.S.Q. c. C-1.1.

JURISPRUDENCE

Prism Hospital Software Inc. v. The Hospital Records Institute (1991), 62 B.C.L.R. (2d) 393 (S.C.).
Tarling v. Tarling, 2008 CanLII 38264 (ON S.C.)
United States of America v Microsoft Corporation 253 F.3d (DC Cir 2001).
Willard v. Caterpillar, Inc., 40 Cal. App 4th 892, 907, 48 Cal. Rptr.2d 607,616 (1995).
William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp.1443, 1455 (C.D. Cal. 1984) & Turner v. Hudson Transit Line, Inc., 142 F.R.D. 68, 73 (S.D.N.Y. 1991).
Zubulake v. UBS Warburg LLC, 216 F.D.R. 280 (S.D.N.Y. 2003)
(1982), 35 O.R. (2d) 164 (Ont. C.A.), affirmed (sub nom. *Bruce v. R.*) [1985] 2 S.C.R. 287 (S.C.C.).

SECONDARY MATERIAL: MONOGRAPHS

Gahtan Alan M.: *Electronic Evidence* (Ontario: Carswell Legal Pubns 1999).
Lange Michele C.S. & Nimsger Kristin M.: *Electronic Evidence and Discovery: What Every Layer Should Know* (Chicago: ABA 2004) .
Rice Paul R.: *Electronic Evidence Law and Practice* (Chicago: American Bar Associations 2005).
Wright Benjamin: *The Law of Electronic Commerce EDI, Fax, and E-mail: Technology, Proof, and Liability* (Boston: Little, Brown & Co., 2nd ed., 1995).

SECONDARY MATERIAL: ARTICLES

Casamassima Thomas J. & Caplicki III Edmund V., "Electronic Evidence at Trial: The admissibility of Project Records, E-mail, and Internet Websites" (2003) 23-SUM CONSLAW 13.
Coumbe G, "E-Discovery" (2004) The New Zealand Law Journal.
Ellis Edward T., "Evidentiary Issues In Employment Cases" (2008) The American Law Institute 1023.
Garrett Cecilia K., "Admissibility of Electronic Information" (2002) 71-SEP.J.Kan.B.A.33.
Haddad Hon.William J., "Authentication and Identification of E-mail Evidence" (2008) 96 ILBJ 252.

Joseph Gregory P., “Trial Evidence in the Federal Courts: Problems and Solutions Sponsored with the Cooperation of the ABA Section of Litigation: Internet and Email Evidence”(2008) American Law Institute 559.
Robins Mark D., “Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation” (2003) 29 Rutgers Computer & Tech. L.J. 219.
Robinson William J., “ An Overview of Electronic Discovery” (2005) Practicing Law Institute 189.
Voigt Romano Leah, “Developments in the Law: Electronic Discovery :VI. Electronic Evidence and the Federal Rules” (2005) 38 Loy.L.A.L.Rev.1745.

OTHER MATERIAL

Beatrice O'Donnell & Thomas A. Lincoln , “Authenticating E-mail Discovery as Evidence” The Legal Intelligencer (13 August 2007) online:Law.com <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1186736525985 >.
Chris Preimesberger, “Intel Faces Up to E-mail Retention Problems in AMD Lawsuit” (7 March 2007), online: <http://www.eweek.com/c/a/Data-Storage/Intel-Faces-Up-to-EMail-Retention-Problems-in-AMD-Lawsuit/ >.
Deb Shinder, “Authentication, Access Control & Encryption: Documenting Authenticity of Evidence for the E-discovery Process” (16 July 2008) online: WindowsSecurity<http://www.windowsecurity.com/articles/Documenting-Authenticity-Evidence-E-Discovery-Process.html >.
Ian C. Ballon, “Spoliation of E-mail Evidence: Proposed Intranet Policies and a Framework for Analysis” Cyperspace Lawyer (March 1999) online: Findlaw <http://library.findlaw.com/1999/Feb/22/131004.html >.
Sedona Canada Principles online:<http://www.lexum.umontreal.ca/e-discovery/The%20Sedona%20Canada%20Principles%20-%20Handout%20Version%202008.pdf >.
X-tech Group: “Email as evidence , ‘Smoking Guns’ Hiding in your Inbox” (2004) online:<http://www.simpsongrierson.com/assets/expertise/xtech/publications/it/2004/KYN_June04.pdf >.