PRACTICE MADE PERFECT CLE BC

ELECTRONIC EVIDENCE
PAPER 3.1

E-Discovery and Privilege: Issues Arising from the Unique Features of Electronic Documents

These materials were prepared by Simon R. Coval and T. Mark Pontin, both of Fasken Martineau DuMoulin LLP, Vancouver, BC, for the Continuing Legal Education Society of British Columbia, October 2007.

E-DISCOVERY AND PRIVILEGE: ISSUES ARISING FROM THE UNIQUE FEATURES OF ELECTRONIC DOCUMENTS

I. Introduction

Electronic documents differ from paper documents in a number of ways material to privilege issues.

In this paper, we explore e-documents and three particular privilege issues:

(1) the difficulty of assessing electronic documents for privilege;

(2) the tension between the high costs of reviewing large volumes of electronic documents for privilege and the risk of inadvertent disclosure without careful review; and

(3) court-imposed sanctions for the improper use of privileged electronic documents.

Electronic documents are created at much greater rates than paper documents and, as a result, there are often much larger volumes of electronic documents available for discovery.[1] In addition to the sheer volume of electronic documents, the number of discoverable documents is increased by the frequency with which information in electronic form is preserved and the ease with which it is duplicated. The following statistics are illustrative: 1) 31 billion e-mails are sent daily; 2) 95% of all company data exists only as electronic documents; and 3) the typical desktop computer includes an 80GB hard drive, which can store the equivalent of 6,400,000 pages of information.[2]

II. Is it Privileged?

Electronic documents raise particular privilege issues, and in some instances electronic documents do not fit comfortably within the traditional categories of privilege or the analysis for establishing

---

1 *The Sedona Canada Principles* (Public Comment Draft). *The Sedona Canada Principles* is the work of Sedona Canada, Working Group 7, which is a public policy think tank based in Sedona, Arizona, dedicated to the advanced study in the law of complex litigation, antitrust law, and intellectual property rights.

2 Paine Hamblen and Jason Pistacchio: *E-Discovery: Everything You Wanted to Know But Were Afraid to Ask.* (ALFA International Conference: *E-Discovery Strategies and Document Retention From The Inside Out*, Seattle Washington, September 19-20, 2007).

privilege in the case law. Two such issues which are addressed in this paper are: 1) whether electronic documents have the requisite confidentiality for privilege to attach; and 2) whether metadata embedded within otherwise non-privileged documents can be protected by privilege.

A. Confidentiality

A reasonable expectation of confidentiality is an essential component of legal advice privilege and also relevant, though of less prominence, in lawyer's brief and litigation privilege.

Electronic documents are not generally consolidated in one location, but often reside in numerous locations: desktop computers, blackberries, laptops, network servers, etc. They are often accessible to individuals who were neither the document's author nor intended recipient. The most common example is network servers, where documents are stored and shared communally, and often third party service providers facilitate and maintain servers used for the storage and transmission of electronic documents and have access to the documents. Martine Bouret and Troy Harrison, in their paper "E-mail Confidentiality and Solicitor-Client Privilege Issues," describe the situation for e-mail:

> The essential problem with e-mail over the Internet is that it does not go directly from the sender's computer over the land-based line to the password-protected mailbox of the recipient. Instead, what usually happens is that the message is sent to the nearest intermediate computer where it is copied into the secure memory of that computer. Once the message is received and stored, the intermediate computer sends a message back to the originating computer that the e-mail was successfully received. This cycle repeats itself, sending the message to the next nearest intermediate computer, until the message finally arrives at the recipient's computer. The message may be sent as one block of data to each computer in the chain or it may be broken down into 'packets' of data which travel along several paths to the final destination. In other words, the e-mail is received and stored by a number of computers on its way across the Internet from the sender to the recipient.
>
> An Internet e-mail message could be intercepted while it is temporarily stored in one of these intermediate computers. Perhaps even more significant is the fact that an Internet provider may intercept, disclose or use e-mail sent through its system to the extent necessary to render the service or protect its rights.
>
> The first problem is that the transportation of the message may allow outside parties to illegitimately intercept and read the message. Anyone who can gain access to any of the computers through which the message is travelling may be able to capture some or all of the message. Given the inherent frailties in the system, communication by e-mail cannot reasonably be expected to afford any significant degree of privacy. Interception may be late to date, but with the increasing use of e-mail there may be greater opportunities and incentives in the future.
>
> The second, and perhaps greater, problem is that as the e-mail travels from computer to computer it is temporarily stored on each machine. The owners of those machines are generally not parties to the communication, have no contractual relationship with the communicating parties, and have every right to maintain their computer systems—which may require opening e-mails from time to time.[3]

Despite these technological facts, the current trend is towards viewing e-mail as sufficiently private for privilege to attach. The BC Law Society has indicated that a lawyer's obligation to keep his or her client's information confidential can be satisfied when using the Internet. The Law Society has stated:

---

3 Martine Bouret and Troy Harrison. "E-mail Confidentiality and Solicitor-Client Privilege Issues" (2003) 26 *The Advocates Quarterly* 23.

> ... [W]hile initially there seems to have been much debate on this topic, the better view today is that there is no basis to conclude that Internet communications are any less private than those using traditional land-line telephones. There does not seem to be a ready and apparent danger that e-mail is less confidential than fax machines or cellular telephones, so anyone using the Internet to communicate has a reasonable and justified expectation of privacy, and it cannot be said as a simple rule that a lawyer must encrypt anything that the lawyer believes the client would not want to read in the local newspaper.
>
> ... [L]awyers communicating on the Internet without encrypting their transmissions do not violate the principle of confidentiality. While encryption makes theft or interception more difficult, even strong encryption can be technically defeated. The vulnerability to theft and interception therefore remains. However, in ordinary circumstances, a lawyer is not expected to anticipate the criminal activity of theft of solicitor-client communications on the Internet any more than mail theft.
>
> The use of e-mail and other electronic media presents opportunities for inadvertent discovery or disclosure of messages, given the manner in which information:
>
> 1. is transmitted within the network systems of an Internet;
>
> 2. is kept as a permanent record if conscious efforts are not made to delete those messages and thereby destroy the prospect of discovery or inadvertent disclosure.
>
> A lawyer using such technologies must develop and maintain a reasonable awareness of the risks of interception or inadvertent disclosure of confidential messages and how they can be minimized.[4]

In *R v. Weir*, [1998] A.J. No. 155, the Albert Court of Queen's Bench considered whether a search warrant issued on the strength of information provided by an Internet Service Provider ("ISP") concerning the accused's e-mail account could be upheld. The ISP, while conducting a routine repair of the accused's account, discovered material which appeared to be child pornography and notified the police of those findings. The Court addressed whether e-mail could carry a reasonable expectation of privacy given that typically ISP's access e-mail for the purpose of routine repairs. In the result, the Court was satisfied that e-mail, though less confidential then other forms of communication, carries a reasonable expectation of privacy.

A more difficult issue arises when third parties have access to electronic documents for broader purpose than ensuring the storage and maintenance of the server within which the document is stored. This arises in the case of company servers where documents are shared communally and the employer has a broad right of access, or simply where computers or e-mail accounts are shared by more than one individual. In such circumstances, questions arise about whether those documents are sufficiently confidential to attract privilege.

This issue was addressed regarding a shared e-mail account in *Dublin v. Montessori Jewish Day School of Toronto*, [2006] O.J. No. 974. The Court considered whether an e-mail sent from the chair of the defendant school's board to counsel was privileged. The e-mail had not been sent from the chair's own computer, but rather she had used her husband's e-mail account. The Court concluded that the e-mail was privileged as "by its very language" it was intended to be kept confidential.

On appeal, the chamber's judge's decision was overturned on other grounds. However, the Court upheld the decision that the e-mail was sufficiently confidential:

> Next, the Dublins argued that given the circumstances of its creation, the e-mail was not intended to be confidential or the confidentiality was waived intentionally or recklessly and thus the e-mail message does not qualify as privileged.

---

4 Federation of Law Societies of Canada: *Guidelines on Ethics and the New Technology.*

> The master made findings of fact against these contentions. (See paragraphs 20 to 22 of her endorsement.) In my opinion, the master did not err in these findings.

(The findings of fact referred to were: 1) that the e-mail was not disclosed to anyone, and 2) that there was no evidence that the chair's husband had actually read the e-mail.)

Reasonable people can disagree about this outcome. As one commentator put it, "it is difficult to reconcile the fact that the e-mail was sent from an e-mail account belonging to a third party (and to which that third party obviously had access), with the court's finding that the sender intended the communication to be kept confidential."[5]

Our courts will no doubt face numerous technologically complex factual situations when adjudicating claims of confidentiality and electronic documents.

B. Metadata

Metadata is information about a particular electronic document that a computer uses to file and retrieve the data. This information does not appear on the face of the document itself, and in many instances is not available or accessible to the computer user. As explained in the *Sedona Canada Principles*:

> Metadata includes information on file designation, create and edit dates, authorship, and edit history, as well as hundreds of other pieces of information used in system administration. For instance, e-mail metadata elements include the dates that mail was sent, received, replied to or forwarded, blind carbon copy information, and sender address book information. Similarly, office documents contain metadata tracking the dates of creation, modification and printing. Internet documents contain hidden data that allow for the transmission of information between an internet user's computer and the server on which the internet document is located.[6]

Metadata is unique to electronic documents. Determining whether metadata is privileged or even capable of being privileged may in some situations prove difficult, as the information does not always fit comfortably within the traditional privilege analysis.

In many instances, metadata will not be relevant to a dispute and it will not need to be produced. There are, however, situations when such information will be relevant (e.g., the authorship and date and time a document was edited could clearly be relevant in a breach of confidence case involving trade secrets),[7] or really any case where fine chronological, editing or authorship issues arise surrounding the document.

In *Desgagne v. Yuen*, [2006] B.C.J. No. 1418, a personal injury claim, the Court considered whether metadata was producible at all. The defendants sought to obtain metadata from the plaintiff's computer to determine what Internet sites the plaintiff had visited and for what duration, claiming this went to the plaintiff's functionality post-accident. Myers J. made the following comments about the nature of metadata and its discoverability:

> The first question to be addressed is whether the metadata is a document. The plaintiff does not appear to take issue with the defendants' position that the metadata is a document.

---

5 Jonathon G. Penner and Graham J. Underwood: *The Latest e-Discovery Case Law Developments and Their Implications.*

6 *Sedona Canada Principles, supra.*

7 *Sedona Canada Principles, supra.*

> The definition of document in the Rules of Court is given an expansive meaning by Rule 1(8), which states:
>
> > 'document' has an extended meaning and includes a photograph, film, recording of sound, any record of a permanent or semi-permanent character and any information recorded or stored by means of any device.
>
> The information being sought does not fit the ordinary or intuitive concept of a document, electronic or otherwise. What is being sought by the defendants is a report of recorded data (i.e., the metadata) that is generated by computer software. That data is not something created by the user, but it is based on what the user does with her software. It is not something that has content in the same sense as a document file generated by the user, for example, a word processing document or spreadsheet. Nor is it something which is printed out or e-mailed in the ordinary course. The assistance of an expert is required to generate the metadata report. In spite of this, it appears clear that the metadata is 'information recorded or stored by means of [a] device' and is therefore a document under Rule 1(8).

Ultimately the Court concluded that the metadata was not relevant and therefore was not to be produced.

In *Spar Aerospace Limited v. Aerowerks Engineering Inc.*, [2007] A.J. No. 974, the Alberta Court of Queens bench considered an application for metadata. The plaintiff alleged that certain employees had copied and taken its technology and claimed damages for breach of contractual and fiduciary duties. The Court, relying on *Desagne,* concluded that metadata was a "record" for the purpose of discovery and ordered that it be produced:

> While metadata presumably need not be produced in most situations, because it is irrelevant to know, for example, when a document was printed, the production of such records is material and relevant here where the pleadings disclose that the identity of the author of electronic records, the timing of the treatment of those records—including if and when they were modified, the dates and tracking routes of e-mail—are all potentially at the very core of the issues raised in the litigation.

Given that the current approach is to treat metadata as a document, privilege issues will arise. For example, privileged information may be disclosed by authorship and edit history.

We are unaware of cases addressing these issues. In our view, in most cases of metadata disclosure, there will be a strong argument of inadvertence and the privilege will be maintained. This topic is considered in the next section.

III. Inadvertent Disclosure

Contrary to older law, recent cases support no waiver of privilege where disclosure was inadvertent. See, for example, *Fording Coal Ltd. v. United Steelworkers of America* (1998), 65 B.C.L.R. (3d) 236 (S.C.); *Pacific Northwest Herb Corp v. Thompson*, [1999] B.C.J. No. 2772 (S.C.).

In some circumstance, however, the risk remains that inadvertent disclosure can amount to waiver. For example, in *Nova Growth Corp. v. Kepinski*, [2001] O.J. No. 5993 (S.C.J.), the Court adopted the following passage from Sopinka, Lederman and Bryant's *Law of Evidence in Canada*:

> Where the disclosure of privileged information is found to have been inadvertent, recent Canadian cases have chosen not to adhere to the principle in *Calcraft v. Guest*, holding that mere physical loss of custody of a privileged document, does not automatically end the privilege. With rules of court now providing for liberal production of documents, the exchange of large quantities of documents between counsel is routine and accidental disclosure of privileged documents is bound to

> occur. A judge should have a discretion to determine whether in the circumstances the privilege has been waived. Factors to be taken into account should include whether the error is excusable, whether an immediate attempt has been made to retrieve the information, and whether preservation of the privilege in the circumstances will cause unfairness to their opponent.

In *Metcalfe v. Metcalfe* (2001), 198 D.L.R. (4th) 318, the Manitoba Court of Appeal concluded that privilege was lost after inadvertent disclosure of a privileged communication because it was important to the outcome of the case and there was no reasonable alternative form of evidence. Further, there is the potential that a court will find that the disclosure of the documents "approached a level of carelessness that was greater than inadvertence."[8]

These principles lead to the risk that privilege can be lost in the exchange of voluminous electronic documents given the prohibitive cost of pre-production review.

A. Clawback and Quick-Peek Agreements

One means of limiting the cost of a privilege review without risk of waiver is agreements with the opposing party prior to disclosure. Two forms of agreement intended to serve this purpose are "claw-back" and "quick-peek" agreements:

> Clawback and quick-peek agreements are becoming increasingly popular in litigation as methods of preventing waiver of privilege through inadvertent disclosure. Clawback agreements are written agreements wherein each party agrees that inadvertent disclosure will not waive the right to claim privilege if the party producing the privileged information request within a reasonable time that the receiving party return the information. This type of agreement allows the parties to disclose documents after a privilege review with the confidence that ether party may promptly demand the return of a privileged document that is inadvertently disclosed. Further, the receiving party agrees not to use the privileged information in the litigation.
>
> In a quick-peek agreement, the parties agree that the requesting party will be allowed to see all of the producing party's information before production including information that may or may not be privileged. The requesting party then provides the producing party with a description of all of the relevant information included in the information viewed, and the producing party exercises any privileged information from the information determined to be relevant by the requesting party. This type of agreement thus eliminates any prior review on behalf of the producing party.[9]

A question arises whether such agreements are consistent with a lawyer's professional obligations to the client to maintain confidentiality of privileged communications. Presumably, these agreements shall only be made under clear client instructions. Another problem is that, though the privilege is protected, the opposing party will have learned something about its existence and nature which may be useful to them in the litigation.

The fact that the documents allow for the return of privileged documents does not negate the potential for prejudice to the disclosing party, as it may be impossible for the opposing party to disabuse their mind of what was contained in the documents, and not to use it to their advantage, even if the documents are not admitted as evidence in court.

---

8 *Chan v. Dynasty Executive Suites Ltd.*, [2006] O.J. 2877.

9 Kindall C. James. "Electronic Discovery: Substantially Increasing the Risk of Inadvertent Disclosure and the Cost of Privilege Review," 52 *Loyola Law Review* 839 (2006).

In *Air Canada v. WestJet Airlines Ltd.*, [2006] O.J. No. 1798, the Court considered whether the use of a quick-peek agreement should be adopted by the court. Air Canada brought a motion for an order confirming that, if any privileged documents were inadvertently produced, such production would not constitute a waiver of privilege, and such production would not constitute an admission of the relevance of those documents.

Prior to the application, Air Canada had produced more than 10,000 documents, but said that it had approximately 75,000 additional documents to produce. The parties had agreed upon search terms to be used to search Air Canada's electronic database. Air Canada proposed to produce the resulting electronic documents without further review of the documents either for relevance or for privilege or confidentiality on the basis that such a review was too costly and laborious. The Court dismissed the application as follows:

> Air Canada says that its proposed manner of proceeding is consistent with Principle #10 [of the 'Guidelines for the Discovery of Electronic Documents in Ontario'] and should be endorsed by this court. I do not agree. I accept that the first stage of Air Canada's approach was appropriate, that is, the use of electronic search terms to identify the apparently relevant documents. WestJet does not dispute this. I do not accept, however, that Air Canada's intention not to conduct a manual review of the resulting documents is validated by Principle #10 nor is it consistent with the requirements of the *Rules of Civil Procedure*.
>
> In my view, it is clear from the Commentary to Principle #10 that some form of further review is contemplated after the electronic search has been completed. The Commentary expressly refers to a 'detailed review for relevance and privilege.' While the Commentary does not expressly say that such a detailed review must be a manual review, and while I am prepared to accept that in some cases such a detailed review might possibly be conducted electronically, in the circumstances of this case, I do not see how that detailed review could properly be accomplished other than manually. I agree with counsel for WestJet that electronic searches alone cannot distinguish between documents that use a word in a relevant context over documents that use the same word in an irrelevant context since words have different meanings in different circumstances. For example, one only has to look at a search term such as 'capacity' to realize that it could be found in an operational document dealing with passenger capacity and also be found in a human resource document dealing with the capacity of an individual to perform his or her duties.
>
> I also agree with counsel for WestJet that solicitor and client privilege is too important a principle for the court to approve of a process that, on its face, has a very large potential for the disclosure of privileged material. Solicitor and client privilege is fundamental to the justice system in Canada - see *R. v. McClure*, [2001] 1 S.C.R. 445 at para. 2. It is not a principle that should readily be sacrificed to the interests of expediency or economics...
>
> ... [G]iven that the state of the law in Canada may not be entirely free from doubt on this point [that inadvertent disclosure may constitute a waiver of privilege], I do not disagree with the general proposition that courts should consider entering such orders in appropriate circumstances. Before doing so, however, one would hope that there would be a consensus among the parties that such an order is necessary. Failing such a consensus, the court would have to be satisfied that the processes adopted by the parties, by which documents are to be produced, would eliminate to the degree reasonably possible the inadvertent production of privileged documents. Absent being so satisfied, the court ought not to lift the normal burden that rests on parties and their counsel to ensure that privileged material is not produced. I will say that I would not consider a process that relied almost entirely on electronic searches and a less than 5% manual review (or a 40% manual review as counsel for Air Canada said at the hearing had now been done) to be satisfactory for this purpose. Rather, such a process appears to be much closer to what is discussed in commentary 10.d. to Sedona Principle #10, as 'clawback' or 'quick peek' production—a practice that is characterized as 'ill-advised' in that same commentary.

The *Sedona Canada Principles* propose a "modified clawback agreement" as a means of meeting the concerns raised in *Air Canada*. Pursuant to a "modified clawback agreement" the parties would undertake a computer word search to identify potentially privileged documents, which would then be removed from the production, with the remainder being produced without a manual review:

> In order for the clawback agreement to be enforceable, the court would likely require prior agreement between the parties that the search methodology would remove from the production set those documents that are potentially privileged. If the search methodology is reasonably thorough, the removal may allow the production of privileged documents to be deemed 'inadvertent' by the courts, and therefore be returned without the loss of privilege. Parties should exercise caution when relying on claw-back agreements because such agreements may not eliminate counsel's obligation to use reasonable good faith efforts to exclude privileged documents prior to initial disclosure. Moreover a claw-back agreement negotiated in one jurisdiction may not be enforceable in another.[10]

Only time will tell if the courts will ultimately embrace and enforce the use of such agreements. If so, they will be an effective tool to minimize cost while protecting privilege.

IV. Sanctions for Improperly Handling Privileged Documents

The increased risk of disclosure of privileged electronic documents is borne not only by the disclosing party but also the receiving party, and the consequences can be grave.

A party in receipt of privileged documents due to inadvertent disclosure that does not amount to waiver of privilege is usually obliged to make no use of the documents, return all copies and any notes containing information from the documents, and keep the information strictly confidential (see *Fording Coal Ltd., supra* and *Chan v. Dynasty Executive Suites*, [2006] O.J. 2877).

The *Autosurvey Inc. v. Prevost*, [2005] O.J. No. 4291decision of the Ontario Court of Appeal is an example of the pitfalls that exist in attempting to employ a "self-help" method for securing another party's documents. The plaintiff obtained unauthorized access to the defendant's computer server and downloaded documents and copied documents, some of which were subject to solicitor-client privilege. As a result of the plaintiff's actions, the Court granted a permanent stay of the action.

In *Chan v. Dynasty Executive Suites Ltd.*, the Court disqualified counsel after they received privileged documents that were inadvertently disclosed in the discovery process. When the disclosing party realized its mistake, it demanded return of the documents. The receiving party, however, refused and instead reviewed them in detail, even though they acknowledged that some of the documents appeared on their face to be privileged. The Court said:

> The case law on this point is clear. Once a lawyer has been advised that privileged documents were produced inadvertently, the lawyer must promptly return the material uncopied and, if possible, unread. If there is any issue as to whether privilege is properly asserted, the obligation of the receiving counsel is to seal the documents, and any notes made in respect of the documents, and seek further direction from the court: *Aviaco International Leasing Inc. v. Boeing Canada Inc.*, [2000] O.J. No. 2420 at para. 11 (S.C.J.); *Nova Growth Corp., supra*, at para.29; *Firemaster Oilfield Services Ltd. v. Safety Boss (Canada) (1993) Ltd.* 2001, 293 A.R. 366 at para. 7 (C.A.); *Williams v. Stephenson*, [2005] B.C.J. No. 1949 at para. 75 (S.C.).

---

10 *Sedona Canada Principles*, at 32.

Such problems have also occurred in the context of Anton Piller orders. E-documents are increasingly the focus of such orders because of the ease with which they can be destroyed by the unscrupulous.[11]

The recent decision of the Supreme Court of Canada in *Celanese Canada Inc. v. Murray Demolition Corp.*, [2006] S.C.J. No. 35 provides a stark example of the dangers that face a party that enlists the powers of an Anton Piller order for the search and preservation of electronic documents without careful consideration of how privileged documents are to be handled.

In *Celanese*, the plaintiff sued Canadian Bearings for alleged industrial espionage. Celanese obtained an Anton Piller order for the preservation and collection of the Canadian Bearings documents, which was executed by an accounting firm and overseen by a supervising solicitor. The Anton Piller order did not make special provision for privileged documents. The defendant's counsel was present at the search but, due to the large volume of documents and the pace at which the search proceeded, did not have time to adequately review for privilege. A number of privileged electronic documents were downloaded by the accounting firm and saved on to a CD-ROM. The plaintiff's lawyers copied them onto its own computers without the knowledge or consent of the defendants. When defendants' counsel became aware that privileged documents were included in the material obtained by the plaintiffs, they sought an order disqualifying counsel from acting.

For the Court, Mr. Justice Binnie stated that:

> Lawyers who undertake a search under the authority of an Anton Piller order and thereby take possession of relevant confidential information attributable to a solicitor-client relationship, bear the onus of showing there is no real risk such confidences will be used to the prejudice of the defendant. Difficulties of proof compounded by error in the conduct of the search and its aftermath should fall on the heads of those responsible for the search, not the party being searched.

Plaintiff's counsel were ordered removed from the proceedings and were ordered not to act or advise the plaintiffs with respect to that proceeding or any related proceeding.

Disqualification of counsel, however, is not always necessary as "in modern commercial litigation, mountains of paper are sometimes exchanged. Mistakes will be made. There is no such thing, in these circumstances, as automatic disqualification." Mr. Justice Binnie noted the following factors as bearing on the determination of whether disqualification is warranted:

> (i) how the documents came into the possession of the plaintiff or its counsel; (ii) what the plaintiff and its counsel did on recognition that the documents were potentially subject to solicitor-client privilege; (iii) the extent of review made of the privileged material; (iv) the content of the solicitor-client communication and the degree to which they are prejudicial; (v) the stage of the litigation; (vi) the potential effectiveness of a firewall or other precautionary steps to avoid mischief.

V. Conclusion

Electronic documents are adding cost and complexity to all aspects of litigation, including protection of privilege.

Many aspects of electronic privilege—confidentiality, the nature of a document, inadvertent disclosure, pre-disclosure agreements, and mis-use of privilege information—are already being tested for our courts.

It is hoped that this paper will assist lawyers as they confront these new challenges.

---

11 Berkely Sells and Ian Collins: *Creative Litigation Solutions to Complex Electronic Evidence Problems.* (Infonex Conference on E-Discovery, Toronto, Ontario, June 2007).