

Technology in Litigation: Friend or Foe
Simon Potter,
Nicholas Trottier, Marc-André Russell
McCarthy Tétrault

Technology in the Courtroom: Friend or Foe
Niagara Falls - August 16, 2010

Canadian Bar Association
August 2010 Niagara Meeting

spotter@mccarthy.ca

Technology in Litigation

- Unavoidable invasion by technology
 - Document management
 - Memory, power, protocol and coding
 - Data recovery
 - Document retrieval
 - Aiding the client
 - Privilege and confidentiality
 - Preparing for the courtroom
 - E-discovery
 - Electronic disclosure
 - E-mails
 - The courtroom itself
 - Lawyers
 - The judge
 - Experts and their reports and testimony
 - Argument
-

“We are so surprised!”

- Clients know that technology has to be used to handle documents and evidence.
 - No client wants to have to hard-copy, 10 times, several thousand documents, and then pay the cost of managing and retrieving that paper.
 - All clients want to get the most out of their documents and to avoid surprises.
 - No client wants the lawyer to use words when a picture will do better.
-

The real world: get used to it

Electronic technology has replaced paper:

- Over 98% of all documents in the commercial world and 100% of legal documents are created, exchanged and stored in an electronic environment.
 - Justice B.T.Granger, Ontario Superior Court of Justice, LEGAL IT 4.0, April 26-27, 2010, Montréal, Québec
-

Electronic Disclosure: disclose what?

“The needle-finding tools have improved, but the haystacks are much, much larger now. Are automated search tools performing well enough for us to use them as primary evidence harvesting tools?”

Unclear on the Concept, by Craig Ball *[Originally published in Law Technology News, May 2005]*

Electronic disclosure: the great power

- Collect documents from numerous sources and locations and submit them to rapid review, collation, organization, display
 - Review and search a company's entire bank of e-mails
 - e.g. receiving 50,000 e-mails in the morning and being able to point to the four key e-mails at an afternoon meeting (CaseLogistix)
 - Collate all documents according to sender, receiver, subject, date or nearly any parameter
-

Protocol and coding: Authenticity Issues

- Date Created
 - By whom
 - Date Last Modified
 - By whom
 - Computer on which created
 - To whom sent
 - Dates printed (?)
-

Protocol, authenticity and chain of custody

To handle an electronic document is to change it.

A competent chain of custody tracks the origins of e-evidence by, e.g., system, custodian, folder, file and dates.

- It is wise to pre-empt attacks on authenticity by preserving complete headers and encoded attachments.
- Be prepared to demonstrate that no one tampered with the data between the time of harvest and its use in court.
- Custodial testimony concerning handling and storage may suffice, but better approaches employ cryptographic hashing of data — “digital fingerprinting” — to prove nothing has changed.

The Path to Production: Harvest and Population (Part III of IV) by Craig Ball
[Originally published in Law Technology News, December 2005]

Data recovery: what if the haystack is lost?

- Back up, and lock away.
- DriveSavers (www.drivesavers.com) and Ontrack Data Recovery (a division of Kroll Ontrack Inc., www.ontrack.com) are the last resort for damaged drives.

Data Recovery: Lessons from Katrina, by Craig Ball *[Originally published in Law Technology News, April 2006]*

Embedded data

Electronic Document

- Created and/or saved in electronic format
- Contains **embedded or hidden data**

Paper Document

- Document never electronic, or
- Copy of electronic document without the embedded data

Exhibit

What to do with embedded data?

E-Mail

“E-mail distills most of the ills of e-discovery, among them massive unstructured volume, mixing of personal and business usage, wide-ranging attachment formats and commingled privileged and proprietary content.

E-mail epitomizes ‘everywhere’ evidence. It’s on the desktop hard drive, the server, backup tapes, home computer, laptop on the road, Internet service provider, cell phone and personal digital assistant. Stampede!”

Cowboys and Cannibals, by Craig Ball [Originally published in Law Technology News, June 2005]

Does e-mail include telephone messages sent by e-mail?

E-Mail: just how far does it go?

Accessible, but Often Overlooked:

- E-mail on remote servers: ISPs (IMAP, POP, HTTP servers), Gmail, Hotmail, etc.
- E-mail forwarded outside: Employee forwards e-mail to personal account.
- E-mail threads: Today's message or all the history of the exchange?
- E-mail threads: Contents (may) diverge from earlier exchanges.
- Offline local e-mail stored on removable media (e.g. memory cards).
- Archived e-mail: Auto-archived or saved under user-selected filename.
- Common "flubs": Users toying with export features and creating e-mail archives.
- Legacy e-mail: Users migrate and "abandon" former e-mail stores.
- E-mail saved to other formats: PDF, .tiff, .txt, .eml, etc.
- E-mail contained in review sets assembled for other (litigation?) purposes.
- E-mail retained by vendors or third- parties (e.g., former service provider).
- Print-outs to paper.

The Path to E-Mail Production (Part I of IV), by Craig Ball [*Originally published in Law Technology News, October 2005*]

E-Mail metadata

Each e-mail is tracked and indexed by the e-mail client: “application **metadata**”.

Every file holding e-mail is tracked and indexed by the computer’s file system: “system **metadata**”.

E-mail metadata helps to establish whether and when a message was received, read, forwarded, changed or deleted.

Williams v. Sprint, 2005 W.L. 2401626 (D. Kan. Sept. 29, 2005), a dispute over production of spreadsheets: the requirement to produce electronic documents kept in the ordinary course of business requires production of **metadata**, barring agreement or protective order.

The Path to Production: Harvest and Population (Part III of IV), by Craig Ball [*Originally published in Law Technology News, December 2005*]

E-Discovery

- Rules of common sense, fed by technological reality
 - Sedona Canada principles: more than just guidance
-

Is it very costly?

“Asked, ‘Is sex dirty,’ Woody Allen quipped, ‘Only if it's done right.’ That's electronic discovery: if it's ridiculously expensive, enormously complicated and everyone's lost sight of the merits of the case, you're probably doing it right.”

The Path to E-Mail Production (Part I of IV), by
Craig Ball *[Originally published in Law
Technology News, October 2005]*

E-Discovery Resources

- Electronic Discovery - A Reading List
 - http://www.practicepro.ca/practice/eDiscovery_RIist.asp
 - E-Discovery Canada
 - <http://www.lexum.umontreal.ca/ediscovery/>
 - The Sedona Conference®
 - <http://www.thesedonaconference.org/>
 - Electronic Discovery Reference Model
 - http://www.edrm.net/wiki2/index.php/Main_Page
-

Sedona Canada Principles

- Electronic information is discoverable.
 - **Proportionality** - Balancing cost and burden of discovery against
 - The amounts at stake in the litigation
 - The relevance and uniqueness of the information
 - Its importance to the court's adjudication
 - Preservation
 - "**reasonable and good faith steps**"
 - "A party's preservation obligation should therefore not require freezing of all electronically stored information, but rather the appropriate subset of electronically stored information that is relevant to the issues in the action."
 - Producing relevant and "**reasonably accessible**" information
 - "marginal utility: Will the quantity, uniqueness and/or quality of data from any particular type or source of electronically stored information justify the cost of the acquisition of that data?"
-

Sedona Canada's 12 Principles

1. Electronically stored information is discoverable.
 2. [T]he parties should ensure that steps taken in the discovery process are **proportionate**
 3. [P]arties should meet and **confer as soon as practicable and on an ongoing basis**, regarding the identification, preservation, collection, review and production of electronically stored information.
 4. As soon as litigation is ... anticipated, parties must consider their **obligation to ... preserve**
 5. The parties should be prepared to disclose all relevant ... information that is reasonably accessible
 6. A party should not be required, absent agreement or a court order ..., to search for ... deleted ... information.
 7. A party may [use] electronic tools ... such as **data sampling** ... to collect potentially relevant ... information.
 8. Parties should agree as early as possible ... on the format in which electronically stored information will be produced. ...
 9. [P]arties should agree to ... judicial direction on, measures to **protect privileges**, privacy, trade **secrets**
 10. [P]arties should ... respect the rules of the forum ..., while appreciating the impact any decisions may have in related actions in other forums.
 11. **Sanctions** should be considered by the court where a party will be materially prejudiced by another party's failure
 12. The reasonable costs of preserving, collecting and reviewing electronically stored information will [normally] be borne by the party producing it. ...
-

Sedona and the “litigation hold”

4. As soon as litigation is ... anticipated, parties must consider their **obligation to ... preserve**
- This is generally held to mean instructions across the enterprise advising
 - there is or will be litigation
 - discovery obligations arise in that litigation
 - **documents meeting certain criteria must not be destroyed or deleted**
-

Sanctions

Pension Comm. of the Univ. of Montreal Pension Plan v. Bank of Am. Secs, No. CIV. 05-9016, 2010 U.S. Dist. LEXIS 1839 (S.D.N.Y. Jan. 11, 2010)

- 13 defendants (5 Québec) **sanctioned**.
 - Found, *inter alia*:
 - Failure to preserve documents or to identify or **alert** persons who should be preserving and failure to stop destruction of e-mails
 - Failure to preserve documents of departing employees
 - Failure to preserve back-ups
 - Ordered:
 - Payment of costs and attorneys' fees
 - Instruction to jury that there had been **spoliation** of evidence and jury could presume the evidence would have been favourable to plaintiff
-

Sedona and claw-back

- *Principe 9: Dans le cadre de l'administration de la preuve électronique, les parties devraient s'entendre ou, s'il est nécessaire, obtenir une ordonnance de la Cour, afin que des mesures soient prises pour protéger les informations privilégiées, les renseignements personnels, les secrets commerciaux et autres informations confidentielles.*
-

Protecting privilege (and confidentiality)

Claw-back arrangements:

I will

- give you all the documents which my search discloses as possibly relevant,
- without taking the five years it will take for me to comb through for privilege and confidentiality,

IF you

- agree that I have not waived privilege or confidentiality, and
 - agree we can debate privilege and confidentiality about any particular needle in the haystack.
-

Claw-back agreements not an excuse for laziness

A claw-back agreement must be viewed using the criteria of proportionality, and is not an excuse for lawyers not to do their jobs or be sloppy or lazy. Manual review can be forced.

- *Air Canada c. Westjet Airlines Ltd.*, 2006 CanLII 14966 (ON S.C.) (para. 15-17)

<http://www.canlii.org/en/on/onsc/doc/2006/2006canlii14966/2006canlii14966.html>

What is a Secret?

« ... Un secret ne demeure un secret qu'en tant qu'il n'est connu que d'un petit nombre de personnes. »

Continental Casualty Co. c. Combined Insurance Co. of America, [1967] B.R. 814,

Varying vulnerability to disclosure of electronic documents

And, therefore, varying treatment of them

- by the courts,
 - by your document management, and
 - by your clawback agreement
-
- How many are there? How many copies of each are there? How many “confidential” copies?
 - How easy is it to copy them? How easy is it to copy a great many of them?
 - Are they programmed to last forever?
 - Have they been through and will they be through many changes? Are they “dynamic”?
 - How many people have handled them? How many of those “forwarded” the documents?
 - How many people mistakenly pressed “Reply to All”?
 - Are the documents reliant on particular softwares or particular platforms?
 - What kinds of policies were in place during the life of the document?
 - Metadata adds to danger.
-

What is the secret? How to protect it.

1. Not all secrets or privileges are the same.
 2. Electronic format adds to danger of unwitting disclosure. Both the precise format and the precise form of the secret affect the degree of danger and the appropriate protective response.
 3. There are different ways of protecting different information.
-

1. Different types of information needing protection

Protocols for document searching and for document disclosure, and claw-back agreements must take into account these differences.

- Professional secrets and privileged information
 - Solicitor-client information
 - Many others
 - Commercial secrets or commercially sensitive information
 - Personal privacy
 - Litigation privileges
 - Documents prepared with a view to litigation
 - Common interest privilege
 - Settlement discussions
-

A number of professional secrets: 45 professions in Québec have “secrets”

ACUPONCTEURS	ADMINISTRATEURS AGRÉÉS	AGRONOMES	ARCHITECTES	ARPEUTEURS-GÉOMÈTRES
AVOCATS ET NOTAIRES	AUDIOPROTHÉSISTES	CHIMISTES	CHIROPATICIENS	COMPTABLES AGRÉÉS
COMPTABLES EN MANAGEMENT ACCRÉDITÉS	COMPTABLES GÉNÉRAUX ACCRÉDITÉS	CONSEILLERS EN RESSOURCES HUMAINES ET EN RELATIONS INDUSTRIELLES AGRÉÉS	CONSEILLERS D'ORIENTATION ET DES PSYCHOÉDUCATEURS ET PSYCHOÉDUCATRICES	DENTISTES
DENTUROLOGISTES	DIÉTÉTISTES	ERGOTHÉRAPEUTES	ÉVALUATEURS AGRÉÉS	GÉOLOGUES
HUISSIERS DE JUSTICE	HYGIÉNISTES DENTAIRES	INFIRMIÈRES ET INFIRMIERS	INFIRMIÈRES ET INFIRMIERS AUXILIAIRES	INGÉNIEURS
INGÉNIEURS FORESTIERS	INHALOTHÉRAPEUTES	MÉDECINS	MÉDECINS VÉTÉRINAIRES	NOTAIRES
OPTICIENS D'ORDONNANCES	OPTOMÉTRISTES	ORTHOPHONISTES ET AUDIOLOGISTES	PHARMACIENS	PHYSIOTHÉRAPEUTES
PODIATRES	PSYCHOLOGUES	SAGES-FEMMES	TECHNICIENNES ET TECHNICIENS DENTAIRES	TECHNOLOGISTES MÉDICAUX
TECHNOLOGUES EN IMAGERIE MÉDICALE ET EN RADIO-ONCOLOGIE	TECHNOLOGUES PROFESSIONNELS	TRADUCTEURS, TERMINOLOGUES ET INTERPRÈTES AGRÉÉS	TRAVAILLEURS SOCIAUX ET DES THÉRAPEUTES CONJUGAUX ET FAMILIAUX	URBANISTES

Particular scope of privilege depends on legislation and jurisprudence. Two examples:

Charte des droits et libertés de la personne, L.R.Q., C. C-12, art. 9

9. Toute personne tenue par la loi au secret professionnel et tout prêtre ou autre ministre du culte ne peuvent, même en justice, divulguer les renseignements confidentiels qui leur ont été révélés en raison de leur état ou profession, à moins qu'ils n'y soient autorisés par celui qui leur a fait ces confidences ou par une disposition expresse de la loi.

Le tribunal doit, d'office, assurer le respect du secret professionnel.

• *Code des professions* (L.R.Q., c. C-26), art. 60.4

60.4. Le professionnel doit respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession.

Il ne peut être relevé du secret professionnel qu'avec l'autorisation de son client ou lorsque la loi l'ordonne ou l'autorise par une disposition expresse.

Doctors a special case

Loi médicale (L.R.Q., c. M-9), art. 42

42. Un médecin **ne peut être contraint** de déclarer ce qui lui a été révélé à raison de son caractère professionnel.

Solicitor-client privilege

- In-house lawyers are covered
Compagnie Montréal Trust c. American Home Assurance Co., [1993] R.D.J. 430 (C.A.)
 - But **not necessarily in other jurisdictions**
 - And **not if the lawyer was giving business advice**
 - And not if the lawyer was really playing a larger role, e.g. President
 - What does this mean for coding of documents prior to disclosure?
-

Privilege: coding methodology

- List of **keywords**
- List of lawyers' names, domain names and other signals to watch out for
- Which of these keywords will **NOT** be useful in filtering for privilege?

ENGLISH	FRANÇAIS
advice	avis
legal	légal
lawyer, attorney	avocat, notaire
privileged, privilege	privilégié, privilège
confidential	confidentiel
solicitor	---
barrister	---
Esq.	maître
LLP	SENCRL

Litigation-related privileges: not necessarily all the same

- Litigation privilege

Blank v. Canada (Minister of Justice), [2006] 2 S.C.R. 319

- covers documents created principally with a view to litigation
- to ensure an efficient adversarial process
 - real, existing litigation
 - threatened litigation
 - settlement of a dispute pre-litigation

- Confidentiality of settlement discussions

- privilege over documents created for the purpose of those discussions

- Common interest privilege

- allows parties to exchange information with a view to forming common strategy in litigation
-

Commercial secrets can also vary

From province to province, and from situation to situation.

Code civil :

1472. Toute personne peut se dégager de sa responsabilité pour le préjudice causé à autrui par suite de la divulgation d'un secret commercial si elle prouve que l'intérêt général l'emportait sur le maintien du secret et, notamment, que la divulgation de celui-ci était justifiée par des motifs liés à la santé ou à la sécurité du public.

2088. Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et ne pas faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail.

Ces obligations survivent pendant un délai raisonnable après cessation du contrat, et survivent en tout temps lorsque l'information réfère à la réputation et à la vie privée d'autrui.

Personal privacy

- Particular statutes
 - Judicial sensitivity
 - Corporate data banks of client information
 - Employees' personal e-mails
-

Facebook: irrelevant that information is on a “private” page

Leduc v. Roman, (Feb. 2, 2009), 2009 CanLII 6838 (C.S.J. Ont.)

(<http://www.canlii.org/en/on/onsc/doc/2009/2009canlii6838/2009canlii6838.html>)

- A party was ordered to disclose his Facebook private profile as it was considered more **relevant** than private.
 - “A party who maintains a private ... Facebook profile stands in no different position than one who sets up a publicly available profile. Both are obliged to identify and produce any posting that relates to any matter in issue.”
-

There is such a thing as a home office, but the office is not your home

- The office computer is not a personal computer.
- There is no reasonable expectation of privacy, especially considering employer's policies re computer use.

Poliquin c. Devon Canada Corporation (17 June 2009),
2009 ABCA 216

(<http://www.canlii.org/en/ab/abca/doc/2009/2009abca216/2009abca216.html>)

R. v. Cole (28 April 2009), 2009 CanLII 20699 (C.S. Ont.)

(<http://www.canlii.org/en/on/onsc/doc/2009/2009canlii20699/2009canlii20699.html>)

Accidental disclosure: accidents do happen

- Is there a “Claw-back Agreement”?
 - Prepared at the outset of disclosure, to facilitate that disclosure
 - Mechanisms for return or destruction of documents
 - Pending judicial decision as to privilege or confidentiality
 - Claw-back is not a panacea: still have to act diligently
 - What if there isn't? Can begging help?
 - How many documents were disclosed, and how quickly?
 - How many turn out to have been privileged or confidential?
 - **What measures were taken to avoid erroneous disclosure?**
 - How long did you wait before reacting to the erroneous disclosure?
-

Sloppiness can make the inadvertent disclosure a waiver of the privilege

- Even in the presence of a claw-back agreement:

Mt. Hawley Insurance Co. v. Felman Production Inc.,
2010 WL 1990555 (S.D. W. Va. May 18, 2010)

Victor Stanley Inc. v. Creative Pipe Inc., 250 F.R.D.
251 (2008)

A poorly conceived or **cursory privilege review risks waiver** when privileged documents are inadvertently produced.

Magistrate Judge Paul Grimm of the U.S. District Court for the District of Maryland, a respected authority on e-discovery.

H. Christopher Boehning and Daniel J. Toal, "[Poorly Executed Privilege Review Can Lead to Waiver](#)," NYLJ, June 17, 2008.

Five factors of reasonableness, even if there IS a claw-back arrangement

- 1) the reasonableness of the precautions taken to prevent inadvertent disclosure;
- 2) the number of inadvertent disclosures;
- 3) the extent of the disclosures;
- 4) any delay in measures taken to rectify the disclosure; and
- 5) overriding interests in justice.

<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202464263612>

“Quick peek” rules

Federal Rule of Evidence 502 in September 2008.

- Responding to spiralling costs of e-discovery, Rule 502 enables litigants to enter into "quick peek" and "claw back" agreements that, **if approved by the court**, enable the parties to limit the need for pre-production review of electronically stored information.
 - H. Christopher Boehning and Daniel J. Toal, "Kansas Case Casts Doubt on Usefulness of Rule 502," NYLJ, Oct. 27, 2009
 - Robert D. Owen and Melissa H. Cozart, "FRE 502: One Year Later", NYLJ, October 13, 2009.
<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202434493885>
-

The courtroom: bringing technology to it, for you

- Having your own computer there
 - On-line?
 - Hook-up to office mainframe?
 - Synchronization of changes to data banks: what if people are making changes at the office while you are making changes in the courtroom?
 - Having your own printer in the courtroom (or next-door)
 - Having paralegals there to code entries (new exhibits, testimony)
-

The courtroom: bringing technology to it, for everyone

- All parties, and the judge
 - seeing the same documents
 - seeing the same transcripts
 - searching through the same data banks
 - All parties, and the judge
 - making their own private marginal notes
 - linking documents to transcripts and vice-versa
 - Particular arrangements
 - choosing the software
 - arranging the hardware (buying it, installing it)
 - teaching the judge
 - uploading daily transcripts and new exhibits
-

Judicial authorization and engagement is key

When?

- Before the commencement of the trial

Who should attend?

- Senior counsel
- Information Technology personnel
- Legal Clerk
- Clients

Justice B.T.Granger, Ontario Superior Court of Justice, LEGAL IT 4.0, April 26-27, 2010, Montréal, Québec

Issues for the Judge to settle

- Will electronic documents and an electronic record suffice?
 - Maintaining the electronic record
 - Will Judge agree to use a litigation support program?
 - Will judge agree to a practice day in the courtroom?
 - Protocol for entering electronic exhibits
 - Courtroom protocol
 - Data backup
 - Software glitches and computer breakdowns
 - Technology support for judge
-

Judge's worries

GRANGER'S RULES FOR AN ELECTRONIC COURTROOM

- **SIMPLE**
- FUNCTIONAL
- PORTABLE
- INEXPENSIVE

Justice B.T.Granger, Ontario Superior Court of Justice, LEGAL IT 4.0, April 26-27, 2010, Montréal, Québec

The courtroom: bringing technology to it, for testimony and expert reports

- We allow tables and graphs created by experts.
 - Why not, for example:
 - Animated “cartoon” illuminating what the data says?
 - For example, a computer-generated animation of a plaintiff’s ride through the defendant’s roller-coaster, showing the G-forces at every turn.
 - Electronic spreadsheet of data allowing the judge to “play” with variables and assumptions?
 - When do you ask for permission to do this?
 - How must such things be handled in appeal records?
-

The courtroom: bringing technology to it, for argument

- Taking the judge through every step in an expert's use of a particular computer program
 - Showing on a screen what happens when an expert's assumptions are changed
 - Showing on a screen what other information was available to an expert
 - Comparing contractual provisions or reviewing e-mail chat
 - Searching data banks, with the judge
-

Technology for judgments

- Embedded extracts from YouTube or pdf's of computer screen captures
 - Dept. of Internal Affairs v. TV Works Ltd., per Judge David Harvey of New Zealand District Court, June 23, 2010
 - <http://www.lawyersweekly-digital.com/lawyersweekly/3013?pg=4&pm=2&fs=1#pg4>
 - http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10657874
 - “Lawyers and judges need to think about **alternative non-textual ways of articulating reasons** for decisions so that the rationale ... is clear, transparent and unambiguous.”
-

Conclusion

- Technology has changed our clients' lives.
 - It has changed what is available as evidence, quantitatively and qualitatively.
 - There is no choice about technology coming into every aspect of trial, of trial preparation and of argument, and eventually of judgments.
 - There is every choice about how.
 - All those choices have
 - advantages and disadvantages,
 - costs and cost savings,
 - particular worries and uncertainties.
-