Computer News for Judges

CNJ

AN ESSENTIAL TOOL: THE CANADIAN GUIDE TO THE UNIFORM PREPARATION OF JUDGMENTS

As electronic publication of judgments becomes the norm, standardizing their format will ensure maximum benefits — for courts, lawyers, publishers and the public.

The Judges Technology Advisory Committee (JTAC), with the help of the Canadian Citation Committee (CCC), has pioneered the dissemination of best practices in preparing judgments and simplifying publication of case law.

Another big step forward is being taken with the publication of *The Canadian Guide to the Uniform Preparation of Judgments*, which

- revises the 1996 *Standards for the Preparation, Distribution and Citation of Canadian Judgments in Electronic Form* and
- integrates the 1999 *Neutral Citation Standard for Case Law*.

All courts and tribunals are invited to implement these standards. The emphasis is on standardizing only the most crucial aspects of judgment formatting, without increasing the workload of staff responsible for judgment preparation. The Guide applies to all judicial decisions from superior courts in Canada and any other court or tribunal that adopts the standards. It sets out best practices regarding the electronic format of judgments distributed in file form.

The Guide reflects a better understanding of electronic documents and the conditions that must be met to use them to their full potential. It improves on and completes the existing standards, emphasizing the standardization of elements required to identify judgments in a searchable database, such as the citation, date and docket number. It is left up to each court to make decisions about the appearance of its judgments.

The Guide's method for naming files gives each file a unique, meaningful name, which makes it easier to manage and distribute. It also sets out standards for processing non-text files, such as pictures, and various kinds of documents issued by courts, such as multiple reasons, versions in different languages, supplementary reasons and corrections to judgments.

As a technical advisor to the JTAC, Professor Daniel Poulin of the Centre de recherche en droit public, Université de

Read about ...

Montréal, is the coordinator of the CCC. He may be reached at (514) 343-2139 or poulind@droit.umontreal.ca. Courts may get direct assistance in implementing the Guide by visiting the CCC's Web site <www.lexum.umontreal.ca/ccc-ccr/index_en.html> or by reaching Frédéric Pelletier, secretary of the CCC, at pelletif@lexum.umontreal.ca or at (514) 343-6111, 1-3257).

Find the Guide at <www.cjc-ccm.gc.ca/english/publications/Guide.en.pdf>.

HIDDEN RISK: THE METADATA PROBLEM IN DOCUMENTS

Documents created by common word processing software such as Word and Word Perfect contain various types of more or less hidden information, called metadata.

Metadata are elements of text added by software to the visible text of a document. They may be as innocuous as formatting instructions. But they may also tell a story of the document's history, including former versions of the text, text fragments removed or added, and reviewers' comments.

Because metadata may be readable by recipients, there is a serious risk of disclosing sensitive information when documents are distributed.

Fortunately, precautions can be taken.

Metadata can be minimized using the features of the word processor that created the document or specialized software that clean documents. Some kinds of metadata are accessible only through what is called a "generic text editor," which can, for example, give access to the last 10 authors of a Word document.

Professor Daniel Poulin and research assistant Frédéric Pelletier of Centre de recherche en droit public, Université de Montréal, have written *The preparation of documents for electronic distribution*, which suggests procedures to deal with metadata issues. The paper recommends procedures for preparing documents for electronic distribution in order to reduce risks related to confidential information and describes software tools that automatically minimize metadata in documents.

The paper is available at <www.lexum.umontreal.ca/citation/guide/en/distribution.en.html>.

SECURITY TIPS: ATTENTION JUDICOM USERS (ESPECIALLY)

In Issue No. 32 of *Computer News for Judges* (Spring 2002) the computer security subcommittee of JTAC offered judges 10 tips on improving security of judicial data. These tips can be found on the Canadian Judicial Council Web site at <www.cjc-ccm.gc.ca>.

Similar advice is now available in more detail, with special relevance to users of Judicom, in *35 Tips on Computer Security*. These tips were prepared by the Computer Education Partnership, a joint project of the Office of the Commissioner for Federal Judicial Affairs and the National Judicial Institute.

The Judicom-specific advice elaborates in particular on the use of Judicom e-mail and the Internet. The tips also go more extensively into password protection and anti-virus protection.

The tips are available at <www.cep.njicourses.ca/comptrng/contents/security_tips.html>.

CORDLESS PHONES AND CELL PHONES: ASSUME YOU'RE BEING OVERHEARD

When Justice Robert Carr travelled Canada as a member of the Judicom training team, to his surprise, he found judges interested above all in the secure use of their telephones! Here is what he told them.

Cordless phones are finding their way into most homes as a convenient alternative to regular wired models. Cellular phones are equally popular. Judges are no exception in their devotion to the cordless/cell trends.

But many judges are unaware that even careful use of these devices exposes them to serious loss of privacy and interception of confidential information.

Cordless phones

Cordless phones and other signal emitting devices such as wireless baby monitors are mini radios whose signals can be picked up by a number of devices, including other phones and scanners. Depending on conditions and equipment, the pickup range can vary from about .5 kilometres to 3 kilometres. Scanners are readily available on the Internet and in some retail stores. They are perfectly legal and cheap to buy, and they're a big seller.

Cell phones

Cellular phones send out radio signals to low-power transmitters, "cells" that are typically 8 to 19 kilometres in radius. In an automobile, for example, as the user travels from cell to cell, the signal is transferred to the nearest transmitter, and in some cases the signal can be picked up by a scanner.

Moreover, a cell phone can be "cloned" with the use of an "ESN" reader; simply, the device reads the phone's electronic serial number and re-programs it into a computer chip on another cell phone, with the result that the thief operates on the victim's phone line.

Minimizing risks

My advice:

- Rule One, of course, is to talk about sensitive matters only on land lines, which are essentially secure.
- Ditch your analog (cordless/cell) phone, period. The analog phone generates a steady uninterrupted signal which is easy to pick up. And don't simply do with it as you might do with your old mattress, namely relegate it to secondary use such as a lake cottage. Replace your analog phones with digital models. Digital phones constantly break up the signal and digitalize it to resist monitoring. And go for quality. You want to ensure at least 2.4 megahertz for quality and distance and insist on DSS (Digital Spread Spectrum) technology which hops from frequency to frequency making it next to impossible to intercept the signal.
- Buy from a knowledgeable retailer and cross-examine him/her on the security issue. If you have chosen a reputable electronics specialist you will minimize your exposure.

Justice Robert Carr is a judge of the Manitoba Court of Queen's Bench and chairs Judicom's Steering Committee.

PERSPECTIVES ON ONTARIO'S INTEGRATED JUSTICE PROJECT

"The Integrated Justice Project in Ontario . . . has not been successful in some major aspects . . . and . . . is now at an end, for all practical purposes."
– Justice N.D. Coo

". . . there are a number of lessons to be learned from the failure of this initiative."
– Justice B.T. Granger

Justices N.D. Coo and B.T. Granger of the Ontario Superior Court of Justice have delivered frank perspectives on the ambitious attempt to create a common electronic environment across Ontario's justice system.

In recent speeches both judges said their judicial colleagues must be front and centre in decisions about the computer technology that will serve their courts in future.

Justice Coo, in a presentation to a panel session of the International Conference on Law via the Internet in Montreal, said the Ontario Integrated Justice Project has "experienced profound financial, business, political and technical difficulties, and will not survive in its present form." Judges were advisors rather than partners in the project and experience has proved that "the bench should not allow such a project to develop without more active and responsible judicial participation."

He said the project's purpose was to create a common and shared electronic database for use by courts, judges, Crown attorneys, lawyers, police and the custodial and correctional system, so that information only has to be noted, created, recorded, stored and archived once, electronically, for criminal, civil and family law matters.

Major problems were encountered in trying to incorporate an Internet-based court case management program, leaving courts without full access to the database, calendaring and scheduling programs or managerial statistics.

Justice Coo said some form of integrated system will come and judges must not let others "either take over what should be the judicial role of court leaders or assume exclusive responsibility for court operations. The judges must be responsible for and fully involved in any new system that will so basically affect the work of the court in almost every way."

Justice Granger, speaking to the Canadian Superior Courts Judges Association in conjunction with the annual meeting of the Canadian Bar Association in London, said the system problems were particularly acute for the Family Court of the Superior Court of Justice, which has adopted case management rules and needed a component that could schedule cases, courtrooms and judges within the rules of case management and circuitry. An attempt to change from a LAN (local area network) based system to a WAN (wide area network) based system was unsuccessful, leaving the courts without the ability to store and retrieve electronic data.

"The initiative also failed as the underlying business case, which was based on immediate staff reduction, was flawed," said Justice Granger. "The introduction of an electronic system will probably not reduce the cost of court service staff in the short term."

Justice Granger said it is imperative that the judiciary independently determine the present and future electronic needs of the court.

"Unless we follow this policy, we will be impairing the independence of the judiciary as we will be outsourcing to others the manner in which we will carry out our responsibilities."

Both judges called for better communication among judicial groups involved in court technology.

COMPUTER MONITORING

Council advises: " . . . computer monitoring of judges . . . must have a well defined and justifiable purpose that does not encroach on deliberative secrecy, confidentiality, privacy rights or judicial independence."

The Canadian Judicial Council has approved guidelines for monitoring court computer systems. These are designed to protect against security threats without compromising judicial privacy and independence.

Developed by the Security Subcommittee of JTAC, the guidelines were approved by the Council's annual meeting in Calgary in late September and have since been sent to all deputy ministers of justice.

The guidelines acknowledge that effective protection of computer networks against security threats requires certain monitoring activities. However, monitoring should have a well-defined and justifiable purpose "that does not encroach on deliberative secrecy, confidentiality, privacy rights or judicial independence," the guidelines state.

The advice grows out of a Council seminar last March led by JTAC, and the work of Professor Michael Geist of the Faculty of Law, University of Ottawa. Professor Geist's paper, entitled *Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance*, is posted on the Council's Web site <www.cjc-ccm.gc.ca>.

Computer Monitoring Guidelines

1. As a general definition, computer monitoring involves the use of software to track computer activities. Monitoring may include tracking of network activities and security threats, as well as Internet usage, data entry, e-mail and other computer use by individual users. Monitoring is done by someone other than the user and may be made known to the user or may be surreptitious. In either case, the user has no control over the monitoring activities and the data that is generated.

2. The effective protection of computer networks against security threats requires certain monitoring activities. However, some types of computer monitoring may represent a significant threat to judicial independence and may also constitute an unlawful invasion of privacy. These guidelines are provided to help judges and system administrators develop appropriate monitoring practices.

3. As an overriding principle, any computer monitoring of judges, and judicial staff who report directly to judges, must have a well defined and justifiable purpose that does not encroach on deliberative secrecy, confidentiality, privacy rights or judicial independence.

4. Content-based monitoring of judges and judicial staff is not permissible under any circumstances. Prohibited activities include keystroke monitoring, monitoring e-mail, word processing documents or other computer files, and tracking legal research, Internet sites accessed, and files downloaded by individual users.

5. In order to safeguard the integrity of shared network resources and protect computer systems against hackers and other security threats, procedures may be implemented for monitoring network traffic, logging errors and exceptions, and performing industry-standard maintenance.

6. Any system integrity and security monitoring must:

   - Be performed only for legitimate network performance or security management purposes.

   - Be the least intrusive approach reasonably available. For example, if network resources are affected by a particular activity, system administrators should try to obtain voluntary compliance by educating judges and judicial staff about specific information technology concerns.

   - Gather aggregate information only. Monitoring computer activity and usage patterns by individual judges or judicial staff is not permissible, except to ensure that users are validly logged in.

7. Monitoring data must be kept confidential. Access must be restricted to information technology personnel who need the information to address system integrity and security issues. Electronic monitoring logs and other records must be purged on a regular basis. Statistical information compiled from monitoring data may be retained, provided it contains aggregate information and addresses system integrity and security issues only.

8. No monitoring may be implemented without the consent of the court's chief justice. Judges and judicial staff must play an integral role in the development and administration of monitoring practices that comply with these guidelines. Any monitoring should be administered by personnel who report directly and are answerable only to the court's chief justice.

9. Judges and judicial staff must be informed of monitoring practices through clear, obvious and consistent notices. Courts should develop acceptable use policies that are communicated when access to computers is first provided. Log-in screens should provide regular reminders about the current policies and the reasons for them.

SECURITY Q & A

by Lewis Eisen & Martin Felsky

Q: I've heard that when you delete a document it doesn't actually get deleted. Is this true?

A: Yes it is true. While you may not see deleted files, they are still very much there.

When you delete a document using typical methods (like dragging it into the Recycle Bin), the disk space that held the file is marked "vacant." The file itself doesn't actually go anywhere. Standard computer programs respond to the "vacant" sign by not including that file when listing the contents of a directory, and so effectively it becomes hidden from view.

The computer doesn't bother cleaning out the data, since eventually the information will be over written by the next file it parks on that space. Until the file is over written, however, it can be retrieved by a file-snooping program, which ignores the "vacant" signs and pokes its nose into each space on the disk to see what's actually there.

This "pseudo-deletion" is supposed to be a feature of the computer, not a bug. Not only does it speed up the deletion process — as you would observe if you ever try to delete hundreds of files at once — but it means that a document deleted by mistake can still be reconstituted. The downside of this "feature" is a security risk: a document that was supposed to have been destroyed can still be examined by prying eyes.

Should you care? Typically, if you are controlling access to your disk, then you can leave the old files lying around and they will be disposed of as the space they occupy gets reused.

If you are planning on selling your computer or otherwise disposing of it, however, you can't afford to leave a trail of crumbs. Before you give up your computer, you should empty the hard disk properly. You will need special software to do this; Norton Utilities, for example, contains a "Wipe" application that cleans up deleted files and file remnants.

The deletion process described in the first paragraph applies to documents and program files that you remove using the delete commands provided by the *operating system* (MS Windows or Macintosh). It does not necessarily apply to e-mail messages or other text deleted using commands provided from within a software program.

Different programs manage deletion and disk space recuperation in different ways. Short of checking the technical documentation for each specific program, you will not know how retrievable your deletions actually are, and even then the documentation may not be clear or entirely accurate.

For greatest security, do not rely on the delete commands of either the operating system or your software programs. Using a disk cleaning utility will erase your data permanently, not just hide it. Only then can you be sure that your documents haven't lingered, to be discovered later by probing eyes.

Lewis S. Eisen, B.A., J.D., is the Senior Trainer — JUDICOM, at the Office of the Commissioner for Federal Judicial Affairs.
Dr. Martin Felsky is President and General Counsel of Commonwealth Legal, Toronto

Computer News for Judges is published for judges by the Judges Technology Advisory Committee of the Canadian Judicial Council. The views expressed are those of the authors and do not necessarily represent the views of the Committee or of the Council.

Computer News for Judges is also available on-line at www.cjc-ccm.gc.ca.