Computer News for Judges

CNJ

JUDGES EXAMINE SURVEILLANCE AND SECURITY ISSUES

The Canadian Judicial Council has endorsed recommendations of the Judges Technology Advisory Committee (JTAC) to put computer security high on the agendas of chief justices and chief judges across Canada, introduce training programs, and create a blueprint of recommended security procedures for all courts.

In the winter of 2000-01, the JTAC Subcommittee on Computer Security carried out a 208-question survey of federal and provincial courts and staff members responsible for court technology. The survey asked about awareness of computer security issues and the priority accorded to them, how security policy is developed within courts, security training, protection of portable equipment, and segregation of judicial and non-judicial computer users.

The results of the survey led JTAC to make a series of recommendations which the Council's Executive Committee approved in November 2001. One of the recommendations asked the Council to devote its March 2002 seminar to computer security issues.

The seminar featured presentations led by JTAC advisors Michael Geist, Professor of Law at the University of Ottawa, and Martin Felsky, President of Commonwealth Legal Inc., and a discussion led by Madam Justice Frances Kiteley, subcommittee chairperson, and Madam Justice Adelle Fruman, a member of the subcommittee.

This issue of *Computer News for Judges* reports on the seminar and offers Dr. Felsky's 10-point primer for individual judges on computer security. The issue summarizes a paper prepared for the Council by Professor Geist on computer surveillance and a new paper on electronic filing and electronic access issues prepared by the B.C. Supreme Court. CNJ also takes a look at developments in court Web sites across the country and some of the plans under way for further refinement of these sites.

Read about ...

TOWARD GREATER COMPUTER SECURITY: JTAC RECOMMENDATIONS APPROVED BY COUNCIL

The report of the Judges Technology Advisory Committee on computer security has been circulated to all chief judges and chief justices, and to deputy attorneys general with a request for their co-operation in implementing the recommendations.

Those recommendations include:

- A request that the National Judicial Institute and the Office of the Commissioner for Federal Judicial Affairs co-ordinate the delivery of training about computer security issues for federal and provincial judges and information technology staff.
- That chief justices and chief judges be asked to establish security of court information systems as a priority, look to early development of security policy in converting to electronic environments, secure resources for security measures, and appoint a technology staff member accountable for security operations.
- Authorization of JTAC to develop a blueprint of recommended security procedures for Canadian courts.

Security Blueprint

The blueprint is to include a protocol that addresses security issues related to the use of notebook computers in court-related travel.

JTAC has also been asked to work with legal and other publishers to establish procedures to avoid release of judgments that contain deleted portions or changes, and to adopt a protocol to withdraw judgments that contain previous deletions or have been released accidentally.

The blueprint, which could also be labelled "best practices" or "minimum standards," will be intended for all courts and all judges, in view of the sharing of networks in many jurisdictions. Similarly, JTAC is recommending that training and some educational programs include both judges and senior technology staff to ensure that all hear the same message.

SURVEILLANCE: NOT A PRETTY SITE?

Professor Michael Geist
Faculty of Law, University of Ottawa

From his paper *Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance*

The ubiquity of computing and Internet communications have catapulted computer and e-mail surveillance to the forefront of public attention. In the workplace, millions of computer-enabled employees who are familiar with their word processing and e-mail applications may know little about surveillance technologies that quietly monitor their network activity, even their every keystroke.

These programs can generate customized reports disclosing how employees use their computers. For example, most surveillance programs monitor the time spent surfing the World Wide Web and provide detailed reports about e-mail activity.

- "Server-based" programs are installed directly onto the employer's computer network and focus primarily on network usage such as e-mail and Internet use. Some can prevent downloading specific types of files such as movies, graphic files or music files.
- "Client-based" programs are installed directly on employees' computers and generate logs of all activities to a file or database for subsequent examination. They can show every keystroke, including those that are subsequently deleted.

Companies of all sizes have begun to install computer surveillance technologies that specifically target employee use of information resources. And not just the mainstream workplace is being subjected to computer surveillance. The U.S. judicial branch was hit by controversy in 2001 when the Judicial Conference of the United States recommended wide-scale monitoring of all computers used by the judiciary and their staff. The matter was finally resolved with the adoption of a modified proposal.

Employer's Right?

It is open to debate whether employers have a legal right to monitor their employees' computer usage. Companies point to several reasons for installing surveillance systems in the workplace.

- To fight employees' personal use of the Internet during business hours. One poll in Canada concluded that employees waste nearly 800 million work hours each year surfing the Internet for personal reasons.
- To sustain network performance. Network efficiency is related to bandwidth and slowdowns caused by employees downloading large audio and video files.
- Liability. Employers may be legally liable for computer misuse, such as copyright infringement and use of unlicensed software.
- Confidentiality and trade secret concerns. Corporations have sustained heavy financial losses from theft of proprietary information.
- Computer crime. Network surveillance may help uncover crimes such as embezzlement and fraud.
- Legal obligation. In certain circumstances, employers may actually have a positive legal obligation to monitor computer usage, for example a requirement for medical companies to protect the privacy of patient information.

The most important source of private sector privacy rights in Canada is the newly enacted *Personal Information Protection and Electronic Documents Act (PIPEDA)*. The law does not take full effect until January 1, 2004, but the principles that underlie it already affect thousands of Canadian organizations.

Emerging case law, statute and policy suggest that a balanced perspective is rapidly emerging in Canada between rights of interception and the right to privacy. Canadian statutes emphasize considerations of the privacy of the computer user, but there appears to be a gradual shift to considerations of the "reasonableness" of computer surveillance.

"Reasonableness"criteria are

(i) Who is being targetted. Consideration must be given to whether or not surveillance should affect all employees equally. Some employees may be accountable for their time through existing reporting procedures. It may not be necessary to monitor employees who do not have access to sensitive data. Some individuals may be monitored only in limited circumstances by virtue of their position; judges are a good example because some forms of surveillance of judges raise both privacy and judicial independence considerations.

(ii) The purpose of the surveillance. Reasons of employee and network performance, liability and trade secret concerns, computer crime etc. were enumerated earlier.

(iii) The prior use of alternatives to surveillance. Arbitration and court decisions have concluded that less-intrusive alternatives to surveillance should be explored first.

(iv) The technology used. Organizations should consider which technology will best serve their purpose while having the most moderate impact on privacy interests.

(v) The notice given the target. In view of the consent exceptions found in the *Criminal Code*, a full informed consent is needed to ensure that workplace surveillance does not breach criminal law.

(vi) Protection of privacy once the surveillance data has been obtained. PIPEDA requires the identification of a point person to address privacy issues within the organization.

An Issue for Judges

The computer has emerged as an indispensable tool for the vast majority of judges. In many provinces, virtually all judges have their own personal computers and use them for a wide range of activities including judgment-related work, communication and legal research.

Judgment-related computer work includes entering trial notes, and drafting and reviewing research memoranda as well as crafting judgments. When several members of the bench participate jointly in drafting a single judgment, collaborative word processing capabilities as well as document comparison functionality are invaluable. E-mail communication is occasionally the medium of choice for highly confidential discussions. Computerized research has become a mainstay of the legal research process.

Judges must consider how monitoring should be instituted in the Canadian judiciary. From international convention and Canadian jurisprudence, it can be concluded that computer and e-mail surveillance of the judiciary is lawful in only the narrowest of circumstances. Monitoring of the content of e-mails and word-processed documents must invariably enjoy full confidentiality. Any surveillance that limits deliberative secrecy would appear to be unlawful. That would likely include the use of client-side surveillance programs such as keystroke logging capable of capturing all data entered into a personal computer.

Professor Geist specializes in Internet and e-commerce law at the University of Ottawa Faculty of Law. He is Director of E-Commerce Law with the Canadian law firm of Goodmans LLP and has written numerous articles and government reports on the Internet and law.

MONITORING: A DAY AT THE COMPUTER

Based on his own one-day experience of research on judicial subjects at the computer, Professor Geist demonstrated what could potentially be monitored, depending on the scope of a surveillance program.

As a judge, you might:	**What monitoring might capture:**
• Boot, log in with the password that connects you to your network.	• Monitoring program can track the log-in.
• Start up word processing e.g. Microsoft Word.	• Identifies use of Word.
• Begin research on insurance law issues in order to draft a memo.	• Reads memo text, including each keystroke.
• Check e-mail, using Outlook Express, and draft e-mail to colleague outside your system.	• Captures text of e-mail, and attachment.
• Start Web brower, go to "CANLII.ORG" for list of cases, correcting your typographical error from CANLII.ORF.	• Captures all Web browsing activity, including search terms.
• Search *Globe and Mail* Web site for cases. Globe gives link to "bad faith insurance.com," which carries class actions against U.S. insurance companies.	• Records all sites you visited, including those you didn't intend to.
• Take a break: check out a reference to TV program called "storefront." Accidentally type "stormfront," which is a hate site.	• Doesn't distinguish between intentional activity and sites visited in error.
• Check out results of U.S. litigation over anti-abortion Web site "Nuremburgfile.com." Automatically sent to "pervertedlinks.com," a pornographic site.	• Monitoring can be set up to show what you are seeing in real time e.g. every 5 minutes, every 10 minutes.
• Try for Supreme Court of Canada site typing "supremecourt.ca," get Web site for B.C. Marijuana Party.	

SURVEILLANCE: SERIOUS ISSUES FOR THE JUDICIARY

Madam Justice Frances Kiteley
Ontario Superior Court of Justice

From her remarks to the Council seminar.

Surveillance of the judiciary's use of computers raises unique and serious issues of judicial independence, impartiality and confidentiality.

A number of court cases suggest that confidentiality of judicial data is crucial to judicial independence.

Judges should expect to have control over the release of their confidential work product, including candid notes about witnesses. They need to be able to research unusual ideas, and to refine their analysis in numerous draft judgments. Nor is there any point in exempting judges from monitoring while at the same time conducting surveillance on judicial staff who share judges' confidential information.

JTAC is preparing recommendations on surveillance of judges and judicial staff in Canada. They will cover outside threats, content monitoring, network performance and other issues.

All chief judges and chief justices need a comprehensive appreciation of the issues arising from the use by judges of computers, and the security of data which judges create. In many provinces the federally appointed judges and provincially appointed judges share the same resources. To the extent that they do, it is important that they pursue a similar approach to security. In any electronic environment, the system is only as strong as the weakest link. JTAC anticipates that all courts in Canada will benefit from its work in establishing a blueprint of recommended security procedures for the courts.

Madam Justice Kiteley is Chairperson of JTAC's Subcommittee on Computer Security

TEN THINGS JUDGES CAN DO NOW TO IMPROVE THE SECURITY OF JUDICIAL DATA

Prepared by JTAC's Subcommittee on Computer Security

1. If you use a notebook computer, treat it with the same care you treat your wallet. Never leave it unattended. Wherever possible, secure your notebook with a cable locking device.

2. Set a "power-on password" on your notebook, and a screen saver password on notebook and desktop computers.

3. Never share your log-in name, user account or passwords with anyone.

4. Choose strong passwords — i.e. not a name or dictionary word. A combination of letters (upper and lower case), numbers and punctuation characters is best. The longer the better. (For example, "Ih2gliO!" is a strong password that is easy to remember. It is the initialism for "I have 2 grandchildren living in Ottawa!") Change your password on a regular basis, for example every 90 days.

5. Make sure key documents and work product are backed up to a server, tape drive, CDs, high quality floppy disks, or other secure and reliable media. Ask your systems administrator to advise you on an appropriate backup procedure.

6. Make sure you use available anti-virus software. Ask your systems administrator to ensure that the virus definitions are updated on a regular basis, and that the software is set to automatically scan floppies, incoming e-mail messages, attachments and downloaded files.

7. If you use Microsoft Word, ask your system administrator to ensure that documents being transmitted outside a secure court environment are free from any hidden information such as revisions and deletions from previous drafts, or private personal information ("metadata"). Provide the system administrator with the following reference information from Microsoft:

- For Word 2000: *How to Minimize Metadata in Microsoft Word Documents* (Knowledge Base Article Q237361). For Microsoft Word 2002, see Q290945, and for Microsoft Word 97, see Q223790. Find Microsoft Knowledge Base

Articles at:
http://support.microsoft.com/default.aspx?scid=fh;EN-CA;kbinfo

8. Use reliable encryption technology to secure particularly sensitive information stored on your computer whether it is being transmitted or not. You may need to ask your system administrator for assistance.

9. When disposing of computers, drives or floppies, use appropriate methods endorsed by your system administrator — for example, all deleted data must be actually purged from storage media and in some cases the media must be physically destroyed. Do not simply "erase" files from a floppy before recycling or reusing it.

10. Monitoring of judges' computer use raises serious issues about privacy, confidentiality and judicial independence. Chief justices should identify the appropriate system administrator and ask for details about the extent to which and ways in which judges' and judicial staff computer use is monitored.

For more information please contact the Subcommittee's Technical Advisors: Martin Felsky, President and General Counsel, Commonwealth Legal, 416-703-3755 x226, mfelsky@commonwealthlegal.com or Jennifer Jordan, Registrar, British Columbia Court of Appeal, 604-660-3237, Jennifer.jordan@courts.gov.bc.ca.

ELECTRONIC FILING: BALANCING OPEN COURTS AND PRIVACY

Chief Justice Donald I. Brenner
Supreme Court of British Columbia

Ms. Judith Hoffman, Law Officer
Supreme Court of British Columbia

From their report prepared for the Administration of Justice Committee of the Canadian Judicial Council, entitled *Electronic Filing, Access to Court Records and Privacy*.

Courts should introduce electronic filing of court records only when they have developed policies that balance fundamental considerations of accountability, privacy and right of access.

Electronic filing and electronic access to court records will greatly increase the efficiency of the courts and the administration of justice. But the new technology will also alter the current balance between the need for open courts and the right of individual citizens to maintain the privacy of personal information. These impacts must be fully considered and protections put in place before systems are implemented.

Current access rules assume that all court records are open to the public except in limited specified circumstances. In fact, the privacy of individuals involved in the court process has been protected by the difficulty, effort and cost of getting at the files. Getting access typically takes a trip to the court registry, retrieval of the file — sometimes from another location — and search fees. Personal information is thus protected by what has been termed "practical obscurity."

Electronic access can change all this. Broad-based searches may be possible from remote locations at the press of a button. Information may be retrieved, downloaded, copied, tabulated and manipulated. The information potentially available may include details of a litigant's work, marital or medical history, date of birth, personal identifiers and detailed financial data. Confidential business information or trade secrets may be required for court records in relation to protective orders.

A contest emerges between individual right to privacy and the right of society to transparency in the administration of justice. In striking a balance, courts should develop access policies that ensure they maintain effective supervisory control over records, and balance three basic values:

- Accountability — the public's right to observe the workings of the justice system and know how and why judicial decisions are made;
- Privacy — the privacy interests of litigants before the court;
- Access — citizens' right of access to the courts to effectively resolve their disputes.

Several basic approaches to access can be taken in developing an electronic filing and access model.

- A "hands-off" approach would maintain current access provisions but place the onus on the litigant to apply for orders sealing files where privacy concerns are at issue. The risk is that individual litigants may lack resources or knowledge to protect their own interests.

- A "take-control" approach places the onus on the court to analyze the information contained in records and remove parts that raise privacy concerns. This would likely require significant increases in court registry staffs.
- A third "user-based" approach would differentiate remote access on the basis of the identity of the person seeking access. This version too places an onus on the court to limit access.
- A fourth model would restrict access based on the type of cases, e.g. criminal cases more restricted than civil; bankruptcy and family cases more restricted by virtue of sensitive financial and identification data.

Whichever model is used, an electronic access policy should consider questions related to the content, form, access to and use of electronic records.

Content questions include whether personal identifiers should be removed and by whom, whether certain types of cases or classes of documents should be excluded from access altogether.

Form of electronic records relates, for example, to whether images of records will be available.

Right of access — will access be extended to the general public over the Internet or limited to registered users and, if so, which ones?

Use of electronic information relates to commercial, research or other purposes not directly connected with the administration of justice, and implies access agreements setting out usage restrictions.

The B.C. Supreme Court has prepared a draft electronic access policy of its own as a basis for consultation with potential users of an electronic filing and access system and with the public. Its seven sections cover types of information that may be accessed, nature of access and searches, security and authentication, service charges, electronic access agreement, access for commercial use and access for research purposes. Each section contains a statement of principle, a policy statement and a discussion of issues involved.

The B.C. report has been sent to JTAC recommending that the committee consider developing a basic model as a guide for courts confronting electronic filing and access issues.

COURTS ON THE WEB

Dramatic changes have been taking place in the number, scope and quality of Web sites operated by superior courts.

Writing in Issue No. 28 of *Computer News for Judges* (http://www.cjc-ccm.gc.ca/english/cnj/cnj_28.htm), (Fall-Winter 1999-2000), Marilyn J. Hernandez and Susan Baer stated:

> There are many reasons why courts want to develop Web sites: to increase access to the courts, the documents, and the process; to increase efficiency of court staff; to reduce duplication and errors in information; and in particular, to disseminate information that already is being prepared by the court in an electronic format.

Issue No. 28 gave this checklist of desirable content for court Web sites:

- Contact or directory information
- Judgments, in a standardized format, fully searchable by a variety of fields using Boolean operators and proximity
- Rules of court
- Court schedules
- Court forms
- Biographies or lists of judges with pictures
- Key court personnel
- Practice directives
- Notices to the profession
- Historical information about the court, judges, the administration of justice in the province or territory
- Overview of each court
- Availability of key documents (e.g. child support guidelines)
- Frequently asked questions, where questions posed by members of the public can be addressed.

The following table illustrates progress to date in incorporating key features from the list.

Progress and Plans for Court Web Sites

	Overview	Contacts	Rules of Court	Forms	Judgments	FAQs	Speeches	Annual Report
Supreme Court of Canada http://www.scc-csc.gc.ca	✔	✔	✔	✔	✔	✔	✔	✔
Federal Court of Canada http://www.fct-cf.gc.ca	✔	✔	✔		✔			✔
Court Martial Appeal Court http://www.cmac-cacm.ca	✔	✔	✔	✔				
Tax Court of Canada http://www.tcc-cci.gc.ca	✔	✔	✔	✔	✔	✔		✔
Newfoundland and Labrador http://www.gov.nf.ca/just/lawcourt/lcourt.htm	✔							
Prince Edward Island http://www.gov.pe.ca/courts/supreme	✔	✔	✔	✔	✔			
Nova Scotia http://www.courts.ns.ca	✔	✔	✔	✔		✔		
Quebec http://www.justice.gouv.qc.ca	✔	✔			✔			
Ontario http://www.ontariocourts.on.ca	✔	✔	✔		✔	✔	✔	
Manitoba http://www.manitobacourts.mb.ca	✔	✔	✔	✔	✔	✔		✔
Saskatchewan http://www.sasklawcourts.ca	✔		✔		✔			
Alberta http://www.albertacourts.ab.ca	✔		✔	✔	✔			
British Columbia http://www.courts.gov.bc.ca	✔	✔	✔		✔	✔		✔
Nunavut http://www.nunavutcourtofjustice.ca	✔	✔	✔		✔			

Nova Scotia's site, launched May 13, 2002, includes a virtual tour of a courtroom as part of its Classroom Project for Teachers and Students. Ontario is considering adding a virtual tour of Osgoode Hall.

The Federal Court of Canada expects to add FAQs, forms and speeches by the end of the summer. The Nunavut Court of Justice anticipates adding FAQs and its annual report.

A court services committee is considering the introduction of a Web site in New Brunswick.

BOOKMARK THESE SITES!

Office of the Commissioner for Federal Judicial Affairs

http://www.fja.gc.ca

Featuring:
- Judicial appointments
- Comprehensive links to federal and provincial court Web sites
- Federal, provincial and territorial legislation

Canadian Judicial Council

http://www.cjc-ccm.gc.ca

Featuring:
- Annual reports
- Issues of *Computer News for Judges*
- Publications, reports and releases
- Council by-laws
- FAQs

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. Contents may be reproduced without authorization provided acknowledgment is made. *Computer News for Judges* is also available on-line at www.cjc-ccm.gc.ca.