Computer Monitoring Guidelines

Recommended by the Judges Technology Advisory Committee, July 2002
Approved by the Canadian Judicial Council, September 2002

[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.