

# SNOOPING IN THE 21ST CENTURY

by Craig A. Zawada

© 2001 Wallace Meschishnick Clackson Zawada

Can employers read employees' e-mail on their computers at work? In Saskatchewan, like most of North America, the answer is a definite "that depends".

Privacy law barely existed 10 years ago but it is now one of the hottest topics for lawyers and the public. There were obvious concerns when computer technology became commonplace, but those worries exploded with the Internet. It was suddenly apparent that personal data could be collected, sorted and distributed instantly.

Since lawmakers do not work at anything approaching "Internet Time", it is not surprising that laws have lagged behind this new technology. Many proposals have been made for privacy laws, but what is the situation today?

Start with the premise that personal privacy has barely been protected in our legal system. There are many reasons for this, but overall, courts felt that a breach of privacy alone was insufficient to ground an action. Different rules applied if the breach led to defamation, or if there was interference with contracts, but privacy alone was not protected.

Especially in the last half century, there were a smattering of cases that did award remedies to someone whose privacy had been infringed. These cases were extremely fact sensitive – they involved situations so unfair and severe that the judge felt compelled to give a remedy, despite the lack of precedents.

Still, there were only a few cases, hardly noteworthy in a legal system which has endured for hundreds of years. Some governments felt that legislation was needed to correct this.

Saskatchewan was a pioneer in this area when they enacted *The Privacy Act*. This Act was intended to kick-start the field of privacy law; instead of replacing the earlier cases, it accepted them, and then added additional remedies.

The Act works by creating a new tort of "violation of privacy" (a tort is a type of action that persons bring for damage suffered, such as nuisance, battery or negligence). Unlike some torts, violation of privacy under the Act does not require the victim to prove he or she suffered any actual damage.

For e-mail, a couple of example torts in the Act apply. It is a tort to conduct "listening to or recording of messages passing by means of telecommunications". Telecommunications would probably include the Internet. One can also not use the letters, diaries or other personal documents of a person.

The Act is not exhaustive, so other privacy violations can occur, but let's just look at these two for now. What impact do they have if an employer looks at an employee's e-mails or computer files?

First, ownership of the computer makes little difference, at least initially. Employers have long argued that they own the systems, and anything the employee does on them belongs to the employer. This might become important when looking at defences later, but the Act's focus is on ownership of the messages themselves, not the medium over which they are transmitted.

Secondly, there is no requirement in the Act that the documents or messages be printed on paper. I am quite confident that a court would see a computer file as a document, even if it can be viewed only on a computer screen.

If we did not go any further then, there could be a strong case against anyone, employers included, who looked at another person's e-mail. As in all torts, however, there are defences that can be raised.

The most common one is consent. Showing that an employee approved the viewing will eliminate the tort. One way of doing this is to enact a company-wide policy regarding use of computers, and the circumstances under which files and mail may be read. It is important to ensure that consent to the policy is explicitly given by existing employees. Just telling them of the new rules may not be enough.

There is no magic in this policy; it can be as simple as "The employer can look at any files, documents or mail on any computer in the office at any time". If the employees agree to this (best to have this in writing), they have consented.

Remember that the Act only adds to the law of privacy; it does not replace it. Therefore, invasions of privacy that are not specifically listed in the legislation can still be actionable.

There are also other defences besides consent. The surrounding circumstances are very important. An internet service provider, for instance, may have to view some e-mail passing through it as part of testing or maintenance. This is unlikely to lead to a privacy tort if the reasons are legitimate.

E-mail is not the only concern under *The Privacy Act*. Other things done by a company can constitute "surveillance". For example, data processing shops often monitor their employees' keystrokes per minute, as a measure of productivity. This could constitute surveillance. Also, security cameras in the workplace would obviously be surveillance. Consider the consequences of this before implementation.

*This article is for general information only and relates only to Saskatchewan law. Specific situations may require different or additional information. Do not act on any information contained in this article without consulting your advisors regarding your specific circumstances. As well, some of the articles are of historical interest only because legislation or case law may have changed.*