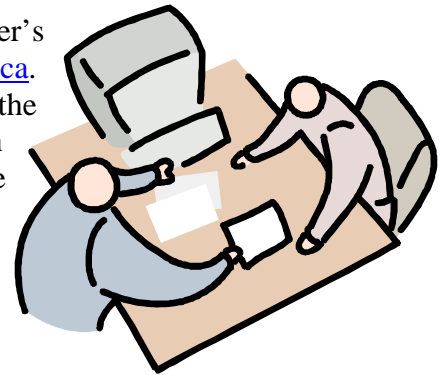


FOIP FOLIO

March-April 2005

Privacy Laws and Health Information: Making it Work!

We are pleased to report that 35 of the presentations from last October's Regina conference are now available on our website: www.oipc.sk.ca. Look under the "What's New" tab. You will have access to the speaker's biographical sketch and if you click on the presentation title, you will have access to either the speaking notes or the Powerpoint presentation of each presenter. You can also still obtain a two disk DVD set with all of the keynote presentations plus some of the workshop presentations through SAHO for \$20 at info@saho.org.



Investigation Report H-2005-002 Prevention Program for Cervical Cancer (PPCC)

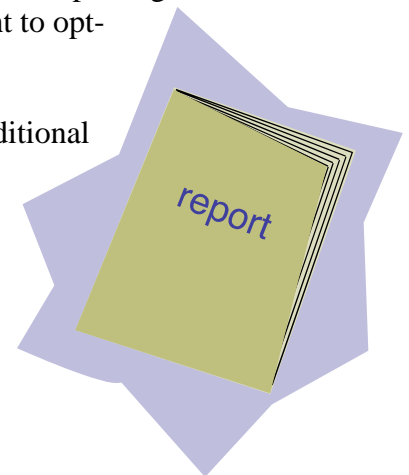
On April 27, 2005 the office of the Saskatchewan Information and Privacy Commissioner (OIPC) released its investigation report dealing with the cervical cancer screening program operated by the Saskatchewan Cancer Agency. The Commissioner has made 19 findings under *The Health Information Protection Act* (HIPA) and offered 25 recommendations. This includes recommendations for Saskatchewan Health, the Saskatchewan Cancer Agency and Saskatchewan physicians.

The Commissioner has also recommended that the Agency go beyond the statutory requirements of HIPA to ensure that any Saskatchewan woman has the right to a full opt-out of the PPCC.

The Commissioner recommends that the Legislative Assembly consider replacing the "no-consent" provision in HIPA with an implied consent (with a right to opt-out) to reflect new Canadian developments in health privacy.

You can access a copy of the full report together with a list of additional resource material online:

http://www.oipc.sk.ca/Reviews_files/Report%20No.%20H-2005-002%20--%20File%20081--2003.pdf



British Columbia Judge Nixes Outsourcing Court Challenge

The Supreme Court of British Columbia issued a decision in March 2005 concerning the attempt by the B.C. Government and Services Employees' Union to stop the contracting out of information management services by the Department of Health Services. In denying the relief the union sought, Justice F.A. Melvin concluded that there had been no breach of the FOIP Act in B.C. or of the *Charter of Rights and Freedoms*.

In his reasons for judgment, Justice Melvin noted that there is an explicit requirement in the B.C. FOIP Act that the public body must make reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal. There is also a requirement that the material must be kept in Canada. In the event there is a foreign demand for disclosure there must be an immediate notification to the relevant minister. As well, the B.C. FOIP Act has created offences and there are penalties for such offences. The judge observed:

Any examination of [FOIP] leads to the conclusion that the government, as previously stated, has done all within its powers to control the dissemination of information and to ensure that the receipt of information by a public body is reasonably secure in the sense that proper precautions have been made to ensure privacy and confidentiality.”

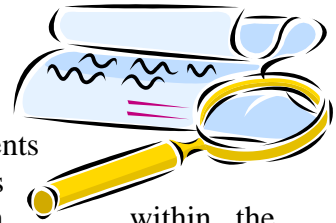
Since our Saskatchewan FOIP Act has none of those features catalogued by the judge, it is interesting to speculate on what a Saskatchewan court would decide in a similar action in this province. The full text of the decision is available at <http://www.courts.gov.bc.ca/jdb-txt/sc/05/04/2005bcsc0446.htm>.

More “Choicepoint” Fallout

Noela Inions of the Alberta OIPC office has brought to our attention a California legislative provision that prescribes mandatory disclosure to individuals of privacy and security breaches. The Ontario Personal Health Information Protection Act also requires disclosure to individuals in the event of an unauthorized use or disclosure. It will be interesting to see whether this is incorporated into other Canadian laws as part of the current reviews underway in Alberta (HIA), Manitoba (PHIA & FOIPPA), PEI (FOIPPA) and the pending review of PIPEDA. Although this is not an explicit requirement in our HIPA, the OIPC recommends that such notification occur as a best practice.

Saskatchewan Report 2005-001

Our office issued this report involving an access request for records of Saskatchewan Labour relating to an industrial accident. The Commissioner upheld the denial of access to certain data elements under the FOIP Act (section 29) but held that the “measured levels of radon exposure of workers” is not personal health information within the meaning of HIPA. Individual levels of radon exposure when linked to employee names should be withheld as personal information within the meaning of section 24. Available online: http://www.oipc.sk.ca/Reviews_files/Report%20No.%202005--001%20--%20File%20029--2004.pdf

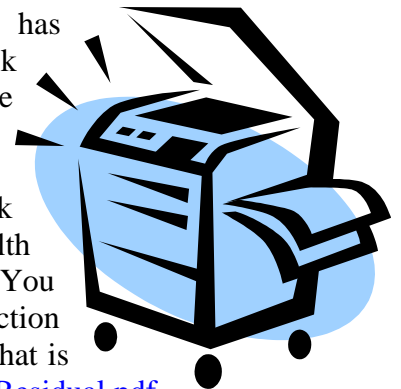


Saskatchewan Report 2005-002

The applicant sought records from Justice with respect to estimates of the Saskatchewan government’s financial liability concerning certain litigation involving the government. The Commissioner found that Justice should have acknowledged whether or not responsive records exist rather than relying on section 7(4) of the FOIP Act. The Commissioner held that the exemption of solicitor-client privilege was well-founded. Available online: http://www.oipc.sk.ca/Reviews_files/Report%20No.%202005--002%20--%20File%20017--2004.pdf

Is your Photocopier / Fax Machine Leaking Confidential stuff?

The Alberta Information and Privacy Commissioner, Frank Work, has produced a very timely caution to organizations about the security risk posed by modern photocopiers and fax machines. Many of these machines will contain hard drives or memory chips. These devices can record and store data that has been photocopied or faxed. When the lease expires or when the machine is serviced or sold, there is a risk of unauthorized access or disclosure of personal information or health information or confidential business information of the organization. You may be particularly vulnerable if you have one of the newer multifunction devices. Mr. Work’s office has produced an excellent Backgrounder that is available at http://www.oipc.ab.ca/ims/client/upload/NR_03_15_2005_Residual.pdf



Major Development at Saskatchewan Justice

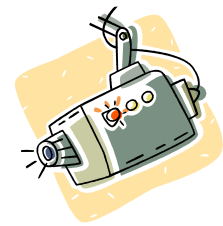
Saskatchewan Justice has been allocated funding in the new budget for a dedicated access and privacy unit. The mandate will be to give advice, develop and provide awareness and educational programming for government employees and develop tools, such as manuals and policies. We are delighted with this development. It is consistent with a number of recommendations made in this office's last Annual Report and our Report on the Overarching Privacy Framework for Executive Government; it assigns responsibility for FOIP training to the Department responsible for the administration of FOIP and LA FOIP (Justice) and it integrates both access to information and protection of privacy responsibilities.

We look forward to working with this new unit. This should be an excellent new resource to assist anyone working for a "government institution" for purposes of FOIP as well as those working for "local authorities".

Video Surveillance Exposed?

In the February 2005 FOIP FOLIO we discussed a United Kingdom report that questions the value of video surveillance as a crime prevention strategy. Now we understand that the Edmonton Police Service has completed a review of the Old Strathcona CCTV Project. The review concluded that the deterrent effect of CCTV could not be disentangled from numerous other factors such as EPS deployment, enforcement, and other EPS initiatives. Published research studies were reviewed and indicated that overall there is no conclusive evidence that CCTV monitoring of city centre streets or public housing leads to a reduction in crime. We understand that the authors found CCTV had a limited role in detecting offences. In most cases, the CCTV was used to observe incidents where police were already on the scene. There was no evidence to suggest that CCTV assisted in police investigations.

These kinds of reports should provide ample reason for public bodies to carefully consider whether video surveillance will in fact make public or private places in this Saskatchewan any safer. We encourage you to consider the Guidelines for Video Surveillance by Public Bodies in Saskatchewan. These guidelines are available at <http://www.oipc.sk.ca/Web%20Site%20Documents/Video%20Surveillance%20June%2024,%202004.pdf>



Pan-Canadian Health Information Privacy and Confidentiality Framework

If you work for a trustee under HIPA, we strongly encourage you to look at the Framework developed by the Deputy Ministers of Health in Canada. This document has been designed as a tool to inform and influence any legislative process within Canadian jurisdictions affecting personal health information. It is the product of extensive analysis and consultation with many organizations including the Saskatchewan OIPC. The objective of this exercise was to harmonize privacy principles governing personal health information throughout Canada.

Curiously, the only two provinces that do not support the Framework are Quebec and Saskatchewan. Our province had participated from the start but then withdrew near the end of the process.

The Framework is available from Health Canada and will shortly be posted on the department website.

‘Steaming open an Envelope’ in an Electronic World

Many of us feel that when we write and send e-mails that it is in fact the equivalent of sending a letter through the mail and believe all contents will remain private between the sender and recipient. On some level, however, we understand that this form of communication is not necessarily as secure from intrusion as we would hope. For instance, at work, you may have a specific policy that details management’s right to monitor this type of communication. Outside of the workplace, those with means and motive may also be viewing your e-mails without your knowledge or permission. This type of interception is already possible through the utilization of a ‘packet sniffer’.

Essentially, a packet sniffer is a program that can see all of the information passing over the network it is connected to. As data streams across the network, the program looks at, or "sniffs," each packet. Usually, a computer looks at packets addressed it while ignoring the rest of the traffic on the network. A packet sniffer wants to look at everything which can be copied and later analyzed. Online activities that may be monitored include:

- The Web sites you visit
- What you look at on the site
- Whom you send e-mail to
- Content of the e-mail sent
- What you download from a site
- What streaming events you use, such as audio and video¹



¹ Available Online: <http://computer.howstuffworks.com/carnivore2.html>

**‘Steaming open an Envelope’
in an Electronic World (cont’d)**

Our Saskatchewan office has been monitoring a new federal initiative proposing to expand the intercept abilities of law enforcement of e-mail and other forms of new communications or technology. This Lawful Access proposal first introduced in 2002 was revisited this March. The proposal included a number of elements relating to the lawful interception of private communications but one of the key requirements is to guarantee that telecommunications providers "*ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies.*"²

The best approach may be to re-evaluate what you send in emails, because you never know who may be intercepting, then reading and using the information gleaned for purposes outside of your control.

Events

May 25, 2005, *First Public-Private Sector Summit on National Security in Ottawa* hosted by Conference Board of Canada. (<http://www.conferenceboard.ca/email/natl-security/default.htm>)

June 15 -- 17, 2005, *Access and Privacy Conference 2005*, University of Alberta at Mayfield Inn, Edmonton, Alberta. (www.accessandprivacy.com for conference details)

To Contact us: Saskatchewan Information and Privacy Commissioner
#100, 1230 Blackfoot Drive
Regina, Saskatchewan, S4S 7G4
Telephone: (306) 787-8350 / Toll Free: 1-877-748- 2298
Fax: (306) 798-1603
E-mail: pscott@oipc.sk.ca
Website: www.oipc.sk.ca

To subscribe to the FOIP Folio, please send your e-mail address to
pscott@oipc.sk.ca

² Silvia Morena-Garci, *Feds Plan to Boost Police Snooping Powers* News Clips from ISPI on *This Terminal City*, March 24, 2005