SIPP Briefing Note

The Saskatchewan Institute of Public Policy

Issue 2, June 2003

Information Management and Privacy Rights:

Are we Adequately Protected Against Intrusion in Our Lives?

The adoption of effective information technology practices is vital for the development of today's knowledge-based economy and society in Canada. Information technology is a source of economic growth and improved public services, and can contribute to an environment where transparency and accountability are two of the most important components of a stable and mutually respectful relationship between government and citizens. However, organizations seeking to derive maximum benefit from information technology must operate in a responsible manner within the scope of existing legislation. It is also important to recognize that the enormous potential of information technology must be constrained by effective regulatory policies, for example, to protect individuals' right to privacy. Governments across Canada have been slow, however, to implement policies and practices that would allow them to effectively manage the personal information in their possession in a way that provides greater access to public records while protecting individual privacy.

Two recent events in Saskatchewan have sparked debate on the issue of privacy protection and prompted the provincial government to review the policies and practices it has in place to ensure that personal information in its possession is adequately protected against unauthorized access and use. In the spring of 2002, six government employees were suspended without pay after it was alleged that they had been providing confidential information to a private investigating company. Several days later, another government employee was suspended after voluntarily admitting involvement. A subsequent internal government investigation confirmed that personal information had indeed been improperly disclosed to a third party and the workers found guilty were disciplined. Upon the completion of the internal investigation, the Deputy Minister of Community Resources and Employment (formerly Social Services), Bonnie Durnford, stated that the government was committed to implementing any changes to its policies and practices that might be needed in handling sensitive information.

Saskatchewan Institute of Public Policy
University of Regina,
College Avenue Campus
Gallery Building, 2nd Floor
Regina, Saskatchewan • S4S 0A2

General Inquiries: 306.585.5777
Fax: 306.585.5780
sipp@uregina.ca
www.uregina.ca/sipp

Furthermore, the Premier assured everyone that the security of the information managed by the government was "good".

However, just a few months later, in January 2003, public concerns about privacy protection surfaced again after a computer hard drive was stolen from the Regina office of ISM Canada, a company that stores large volumes of private and business information for the provincial government. Some of the records on the hard drive included government employee pension statements, applicant information about bulk fuel rebate programs, personal files of Workers' Compensation Board clients, as well as information belonging to the Manitoba Government, the Investors Group and the Co-operators Life Insurance Company among others. This led the province's Privacy Commissioner to begin a review of the government's information security policies and practices in order to determine whether the government was negligent in managing personal information. The stolen hard drive was ultimately recovered by the police and no evidence was found that any information on it had been misused; nonetheless, questions were left unanswered about the government's ability and, more importantly, commitment to ensure that there are adequate safeguards for the protection of sensitive information that is outsourced to third parties.

This Briefing Note examines the privacy legislation and government management practices in Saskatchewan, and provides an analysis of what has been done to protect personal information in the provincial public sector. It presents the conclusions and recommendations of two recent official privacy reviews in an attempt to evaluate the government's performance, based on a number of privacy principles introduced by the Canadian Standards Association (CSA). The paper also makes suggestions about what still needs to be done in order to keep up with the rapid pace of technology advancement and respond to the challenges of the twenty-first century without compromising the legitimate interests of Saskatchewanians, such as privacy protection.

A related issue that will not be discussed here is the protection of personal information managed in the private sector. It may be noted, however, that the federal government has recently enacted supplementary privacy legislation to govern the private sector, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which will apply to the provinces as well, unless they adopt "substantially similar" legislation of their own. Quebec passed such legislation in 1994, which pre-dated PIPEDA, while British Columbia and Alberta have already introduced bills in their legislatures that are waiting to be debated and implemented[1]. Saskatchewan, and all other provinces without private-sector privacy legislation, will fall under the scope of the federal Act from January 1, 2004.

Privacy Legislation in Saskatchewan

In the last decade, Saskatchewan has been at the forefront with regards to access to information and privacy legislation in Canada. The *Freedom of Information and Protection of Privacy Act (FOIPPA)* and the *Health Information Protection Act (HIPA),* the latter of which was passed in the provincial

[1] The Ontario Government has indicated that it would like to have a "made-in-Ontario" privacy legislation, however, no draft has been introduced in the provincial legislature yet.

legislature but will not come into force until all parties affected by it have had adequate time to prepare for its implementation, are the main statutes. The two Acts are among the most comprehensive in the country. They have been designed to facilitate access to public records by citizens, improve information-sharing among government departments and agencies, and at the same time, reduce the risk of illegitimate access, intrusion by government in private and business affairs, and identity fraud.

The *Freedom of Information and Protection of Privacy Act* provides a definition of personal information and sets out the rights and responsibilities of the provincial government in relation to the protection of privacy rights. By and large, the most sensitive information about an individual is managed by the government departments/agencies whose activities involve the administration of personal income tax (Saskatchewan Finance), and criminal and health history (Saskatchewan Corrections and Public Safety, Justice, Health and the Health Information Network). On the other hand, perhaps the largest volume of highly confidential personal information is managed by the Department of Community Resources and Employment.

The *Freedom of Information and Protection of Privacy Act* contains a provision for the appointment of an Information and Privacy Commissioner, whose mandate is to carry out research on matters within the scope of the Act, engage in public education programs, and receive representations regarding the implementation of the Act. After reviewing a case, the Commissioner prepares a report with recommendations and gives reasons for those recommendations. However, a Commissioner's decision is not legally binding and can be appealed in a court of law. Unfortunately, in Saskatchewan, the Information and Privacy Commissioner has not taken on as active a role in privacy protection as in other provinces, due to very limited funding and shortage of staff. In the 2003-04 provincial budget, there is an estimated $306,000 to be provided to the Office of the Commissioner. This figure is negligible compared to Alberta and Manitoba, where the corresponding offices will receive $3,293,000 and $2,296,100, respectively, this fiscal year. Given this small budget and staffing, it is difficult not to conclude that the Office of the Information and Privacy Commissioner, and the issues of access to information and privacy protection in Saskatchewan, are relatively unimportant to the provincial government.

What is Considered Personal Information?

Information that describes an identifiable individual pertaining to "race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual" is legally considered personal. Personal information also includes name, telephone number, home address, social insurance number, education, criminal and health history, financial transactions, tax reports, etc. However, information about salary and benefits of public employees, financial data from public contracts, and licenses and permits is not classified as personal.

The primary activity of the Commissioner so far has been to review requests for access to information or for checking the accuracy of personal information managed by the government; the issue of privacy has only been engaged as a reason to deny access to information. The gap between the role Information and Privacy Commissioners could play in enforcing the *Freedom of Information and Protection of Privacy Act* in Saskatchewan and that which they have played to date, necessitates a bigger budget for that office. The appointment of a new Information and Privacy Commissioner this summer (an open competition to fill in the position is currently underway) provides an ideal opportunity for government to respond to the increased public interest in privacy issues and allocate sufficient resources to the Commissioner's office to fulfill its entire mandate.

Privacy Principles

The main problem governments (not only in Saskatchewan) face in relation to personal information management has been how to balance the protection of privacy rights against other competing interests. Public organizations operate within the scope of existing laws and have a mandate in the economy and society to provide various social programs and services to the general populace. It is a challenge to achieve a trade-off that is acceptable to all parties involved, but governments must make every effort to avoid compromising their responsibility for privacy protection. Therefore, it is important to adopt and enforce appropriate policies and practices for the protection of personal information, which should be reviewed periodically to ensure legislative compliance and consistency with organizational goals.

Canadian Standards Association Privacy Principles

Accountability: an organization is accountable for the personal information it manages and should designate an employee or employees to ensure compliance with the existing legislation.

Identifying Purposes: an organization should define (identify) the purposes for which personal information is to be used before or at the time of the collection of that information.

Consent: an individual must consent to the collection, use, disclosure and retention of his/her personal information except in certain circumstances. Legal, medical or security reasons may make it impossible or inappropriate to seek consent, for example, when the individual is a minor, seriously ill, or mentally incapacitated, as well as for crime prevention or law enforcement. The form of consent (written or implied) depends on the type of information and the purposes for which it is to be used.

Limiting Collection: an organization should limit the collection of personal information to the amount necessary for the identified purposes.

Limiting Use, Disclosure, and Retention: personal information should only be used for the purposes identified by the organization, except with the individual's consent or for law enforcement. Personal information should not be retained for longer than necessary for the accomplishment of its intended purposes.

Accuracy: personal information should be accurate, complete and up-to-date for the identified purposes.

Safeguards: an organization should implement safeguards for the protection of personal information according to the level of sensitivity of that information.

Openness: an organization is responsible for properly informing individuals about its policies and practices with regards to the management of personal information.

Individual Access: an individual should have access to his/her personal information held by an organization, upon request. There are exceptions, however: where it is costly to provide such information, where the information refers to other individuals, or for reason of business or litigation privilege. These exceptions, on the other hand, should be limited and specific.

Challenging Compliance: an individual should have the right to challenge an organization's information security policy or practice with respect to compliance with the applicable privacy legislation.

The Canadian Standards Association's (CSA) *Model Code for the Protection of Personal Information*, which was released in 1996, contains 10 principles of privacy that provide a tool for evaluation of privacy policies and practices. In summary, these principles are: accountability; identifying purposes; consent; limiting collection, use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. The privacy principles can be regarded as vital for the establishment of a comprehensive framework of guidelines for the protection of personal information in today's knowledge and technology-based economy in Canada. The CSA model can be applied in both public and private organizations, because the issues it addresses, such as the collection, use, disclosure, and retention of personal information, and the right of individuals to have access to information about themselves and to ensure that this information is accurate, are not ownership-specific.

Evaluation of Privacy Practices in Saskatchewan

The extent to which privacy rights are protected in Saskatchewan is the primary focus of an official assessment by Deloitte & Touche released in February 2003. This report was conducted at the request of the Saskatchewan Government and presents a comprehensive review of current practices and methods of handling sensitive information in 17 departments and Crown Corporations in the province. It was prepared as a response to increased public concerns about the security of personal information and followed two reports by the Provincial Auditor, in 1999 and 2002, on information technology (IT) security. These proposed a number of urgent recommendations regarding increasing the level of protection of personal information managed by government departments and agencies.

According to Deloitte & Touche, on the basis of the privacy principles embodied in the *Model Code for the Protection of Personal Information*, the Saskatchewan Government has demonstrated that it takes the issue of privacy protection seriously. However, there is still room for improvement of current practices. The 1999 Provincial Auditor's Report identified a number of trends in the development of information system technology that would have an effect on the way the government handles personal information. As the use and sharing of electronic data between organizations have increased, the volume of exchanged information and the complexity of tasks to be performed has grown as well. Networks have become one of the most common tools for the government to manage the information in its possession. In light of these developments, the report underscored the need for enhanced IT security and recommended several steps to be taken

"...the Saskatchewan Government has demonstrated that it takes the issue of privacy protection seriously. However, there is still room for improvement of current practices."

to ensure that the risk of inappropriate use, dissemination, change or destruction of personal information was minimized. The recommendations broadly included: improved employee awareness and responsibility for protecting sensitive documents, greater involvement of senior management in creating and maintaining a safe environment for working with confidential information, and independence of IT security officials from those engaged in IT operations in order to avoid conflict of interest. The 2002 Provincial Auditor's Report followed up on the recommendations made in 1999 and concluded that very little progress had been made within government in their implementation. The 2002 Report made similar recommendations and urged the responsible government officials to take appropriate steps in their departments and agencies to ensure the secure handling of sensitive personal information.

Deloitte & Touche noted in their February 2003 report that none of the departments and Crown Corporations had a designated Privacy Officer, even though in many of them, the person in charge of complying with the *Freedom of Information and Protection of Privacy Act* often informally did that job. A number of organizations outsource the management of their information to third parties, but there is no central oversight of the contracts within the government to ensure that the third parties understand their responsibilities with respect to the protection of personal information. Central oversight could help to avoid privacy breaches, such as the incident with the stolen ISM hard drive. It is common for departments and Crown Corporations to seek only implied consent for the collection, use, disclosure, and retention of personal information, which may not always reflect the degree of sensitivity of the information managed.

Despite the existing safeguards of information, such as confidentiality and appropriate-use policies, they are not routinely applied to ensure adequate and continuous protection. Government employees must be familiar with their responsibilities for protecting the personal information to which they have access. They should be required to formally acknowledge any new or amended departmental policy or memorandum regarding privacy. The privacy breach in the spring of 2002, when government employees disclosed confidential information to a private investigating company without authorization, underscored the need for better employee education and supervision. Last but not least, is the general lack of regular reviews of security arrangements by departments and Crown Corporations. The Deloitte & Touche report concludes that the general level of privacy-rights protection in Saskatchewan is satisfactory, but it also identifies areas where the government needs to improve its performance to reflect constantly changing privacy practices across Canada.

The transition from paper to electronic processing of requests for information in recent years has created new challenges for legislators and public servants, the most significant of which is the balancing of access to records by both public officials and citizens with the right to protection of personal information. The increased flow of information among government departments and

agencies, and to third parties, makes it imperative to put restrictions on the amount and details of information that is accessed and exchanged. Each department and agency should possess, manage, and have access only to personal information that is necessary for the fulfillment of its mandate, which is not presently the case in Saskatchewan. There is too much sensitive information being collected and stored electronically within the government, which is disturbing. Why should, for example, SaskTel and SaskPower, and possibly others, possess individual social insurance numbers? This type of information should be necessary only for the branches of government that deal with personal income tax or pension matters, or law enforcement, such as the provincial Department of Finance and the Department of Justice. The collection and exchange of non-essential information between organizations (including the private sector) only increases the risk of unauthorized access or disclosure of personal information.

In conclusion, all government departments and agencies in the province have a legal duty to manage personal information as prescribed in the *Freedom of Information and Protection of Privacy Act*. They are expected to handle such information in a responsible manner by ensuring accuracy, and providing and reviewing periodically the necessary safeguards against unauthorized and unlawful access, use and dissemination of personal information. In today's increased sharing of information among organizations, it is vital that the government create and sustain a secure environment for information access and exchange. Unfortunately, while there are encouraging signs, there is still room for improvement in Saskatchewan.

Our Author: Pavel Peykov, *SIPP Policy Analyst*
Pavel Peykov joined the Institute during the summer of 2002. He was previously employed with Saskatchewan Energy and Mines and the University of Regina. Mr. Peykov's education includes a Bachelor of Arts (Honours) in Business Administration from the University in North London, London, England and a Master of Arts in Economics from the University of Regina. He is currently working towards a Master of Public Administration from the University of Regina. For further information, please call Pavel at (306) 585-5862.

SIPP Briefing Note

The **SIPP Briefing Note** series allows the Institute to review and comment on public-policy issues that affect the people of our community. A **SIPP Briefing Note** will be released several times a year and can be used as an instrument for further discussion and debate. The first issue of the **SIPP Briefing Note,** released December 2002, explored the issues surrounding automobile insurance within Saskatchewan, specifically since the introduction of the alternative tort option.

The Saskatchewan Institute of Public Policy

www.uregina.ca/sipp

The **Saskatchewan Institute of Public Policy** (SIPP) was created in 1998 as a partnership between the University of Regina, the University of Saskatchewan and the Government of Saskatchewan. It is, however, constituted as an institute at the University of Regina. It is committed to expanding knowledge and understanding of the public-policy concerns in Canada with a particular focus on Saskatchewan and Western Canada generally. It is a non-profit, independent, and non-partisan Institute devoted to stimulating public-policy debate and providing expertise, experience, research and analysis on social, economic, fiscal, environmental, educational, and administrative issues related to public policy.

The Institute will assist governments and private business by supporting and encouraging the exchange of ideas and the creation of practical solutions to contemporary policy challenges. The Founding Partners intended the Institute to have considerable flexibility in its programming, research, contracting and administration so as to maximize opportunities for collaboration among scholars in universities and interested parties in the public and private sectors.

The Institute is overseen by a Board of Directors drawn from leading members of the public, private and academic community. The Board is a source of guidance and support for SIPP's goals in addition to serving a managerial and advisory role. It assists SIPP with fostering partnerships with non-governmental organizations, the private sector and the expanding third sector.

Saskatchewan enjoys a long and successful tradition of building its own solutions to the challenges faced by the province's citizens. In keeping with this tradition, the Saskatchewan Institute of Public Policy will, in concert with scholars and practitioners of public policy, bring the best of the new ideas to the people of Saskatchewan.

Saskatchewan Institute of Public Policy
University of Regina, College Avenue Campus
Gallery Building, 2nd Floor
Regina, Saskatchewan • S4S 0A2

General Inquiries: 306.585.5777
Fax: 306.585.5780
sipp@uregina.ca
www.uregina.ca/sipp

UNIVERSITY OF REGINA