Global Information Assurance Certification Paper

Effect of the Personal Information Protection and Electronic Documents Act on Computer Security in Canada

Robert Lockrem

GSEC v1.3

The Personal Information Protection and Electronic Documents Act first came into effect January 1, 2001, with the final implementation being complete January 1, 2004, and provides a legal basis for the protection of personal information which is gathered in the conduct of commercial activities. This Act is built on principles that place the responsibility for the protection, correctness and limited use of information on the organization, while ensuring that the individual is aware of not only the collection of the information, but also all planned uses.

This has a significant impact on computer security in Canada, not just as outlined within the individual principles themselves, but also combinations of principle requirements have distinct effects. This is the first time that such requirements have the force of law behind them. The legal requirements of the Personal Information Protection and Electronic Documents Act make it mandatory for organizations to have policies and practices which are designed specifically for the protection of person information. To ensure enforcement of the Personal Information Protection and Electronic Documents Act, the Office of the Privacy Commissioner has the full authority to investigate any complaints relating to personal information under the jurisdiction of Bill C6 or suspected violations. Bill C6 also allows Canada to conduct business openly with the nations of the European Union which must abide by the European Union personal information protection laws.

History

In a 1988 poll conducted by Angus Reid, "88% of Canadians polled said that they found it unacceptable for companies and organizations to sell, trade, or share lists containing personal information".[1] In response, Bill C-6 was initiated in the House of Commons. This bill became law April 13, 2000 as the Personal Information Protection and Electronic Documents Act, hereafter referred to as Bill C-6 as this is the more common name for the Act at this time. Bill C-6 contains two distinct sections, Protection of Personal Information and the use of Electronic Documents as legal documents. The second section does not directly impact information security, and will not be reviewed.

At the time of this survey the primary privacy legislation in Canada was the Privacy Act of 1980. The Privacy Act provides the same protection for personal information as Bill C-6; the major difference between these two pieces of legislation being the organization collecting and using the information. The Privacy Act was written to protect personal information gathered by various departments and agencies of the federal government, as defined in Section 3 of the legislation.

The Privacy Act also created the Office of the Privacy Commissioner, tasked with and granted the authority to investigate complaints regarding non-compliance. Specific powers granted the Privacy Commissioner include the authority to issue and enforce

---

[1] Manley, Honourable John. "Third Reading Speaking Notes Bill C-6." January 27, 2001. URL:http://www.ic.gc.ca/cmb/welcomeic.nsf/558d636590992942852564880052155b/85256779007b79ee8525681200667a45!OpenDocument. (January 31, 2002).

summons to individuals when investigating violations of the Privacy Act. Associated with this are the rights to administer oaths, compel individuals appearing at an investigation to provide statements under oath and accept statements and/or evidence related to an ongoing investigation. With regards to investigatory powers, the Privacy Commissioner is authorized to enter any government building, providing site security requirements have been met, interview individuals and obtain copies of documents relevant to the investigation. The Office of the Privacy Commissioner remains a key element of enforcement of personal information protection under Bill C-6 as well.

Implementation

With the implementation of Bill C-6, the Privacy Act remains in effect over the collection of information by the federal government. Bill C-6 contains a three step implementation plan which began on January 1, 2001. The first stage focuses on those organizations considered to be federal works, defined as "any work, undertaking or business that is within the legislative authority of Parliament".[2] This includes commercial undertakings in the areas of shipping, any form of transportation which crosses provincial boundaries, banking or any other endeavor which does not fall under provincial jurisdiction. Information and activities covered by Bill C-6 include the personal information collected in the course of commercial activities, disclosures of information across provincial or national boundaries and personal information collected about employees. Information which is not considered to be personal, and is therefore not covered by Bill C-6, includes employee name, title, business address, office telephone number and information collected by individuals for personal use.

Stage two of the implementation came into effect January 1, 2002. This phase covers health information collected by the same organizations covered by Bill C-6 effective January 2001. Personal health information defined by Bill C-6 is any information about a person's mental or physical well being and services or tests provided.

The final stage comes into effect January 1, 2004 and extends the scope of Bill C-6 beyond federal works to include all commercial activities carried out in Canada. Exemptions to Bill C-6 are allowed to organizations in provinces which have passed legislation which meets the test of substantial similarity to Bill C-6. At present, Quebec is the only province to have enacted such legislation, however a number of other provinces and territories are considering privacy legislation.

A number of personal rights to personal information collected by third parties are defined within Bill C-6. These personal rights reflect the obligations set out by the ten principles on which Bill C-6 is based. These rights include knowledge of why information is being

---

[2] Bill C-6. April 13, 2000. URL: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html. (January 30, 2002)

collected and how it will be used*, the expectation for corrections to be made to erroneous information in a timely manner, protection of information by the collecting organization and access to a process to file a complaint regarding the handling and/or use of personal information.

Principles

Bill C-6 has been written around ten principles, as originally outlined by the Canadian Standards Association Model Code for the Protection of Personal Information in 1996. This code was created as a response to the adoption of different privacy codes by industry and the European Union's Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. Bill C-6 is the federal government's method of implementing a standard code of information protection which is comparable to the privacy requirements being implemented in other countries.

Accountability: The principle of accountability creates the legal obligation for organizations to secure all personal information collected. This responsibility is fulfilled at four different levels. At the highest level, organizations are required to comply with all ten principles set out in Bill C-6. Next, policies must be developed which specifically address the collection, handling and protection of personal information. Also, practices and procedures must be implemented to enforce the personal information protection policy. Third, a corporate compliance officer must be appointed. The privacy officer should have the support of management and the access and authority required to act on all information security issues. Both the policy and the privacy officer's name, title and contact information must be freely available. Finally, Bill C-6 makes any organization accountable for the protection and use of any information which is transferred to a third party. This requires any company disseminating personal information to ensure that the information is protected at a consistent level and is only used for the purposes, which the individual gave permission.

Purpose: The purpose for collecting information must be clearly documented prior to collection. This requirement creates an official record which assists in meeting the obligations of five principles, accountability, consent, limited information collection, limited information use and recourse. The purpose for information collection must also be recorded for previously collected information prior to its use. Regardless of the original purpose for the data collection, any use of the information can not occur until permission is granted by the individual to which the information pertains.

Consent: Prior to or at the time of collection, consent for the collection, use and disclosure of personal information must be obtained. When obtaining consent, the reason for the collection and any planned use or distribution must be clearly explained and

---

* Use represents any usage of the information by the collecting organization or distribution to other business units within the same organization or a third party external to the collecting organization, unless otherwise noted.

provision of a product or service can not rely on consent. Once given, a record of consent should be maintained with the data collected and the purpose provided to obtain consent. This will decrease the time required to consent for additional use investigation of a complaint.

Consent is not required in all circumstances. A total of eleven general circumstances demonstrate the five combinations of collection, change of use and disclosure outlined in Bill C-6 for which consent is not required. Consent is not mandated when knowledge of information collection, use or disclosure by the individual the information is about may negatively impact the validity of the information collected and the information is to be used for investigation of a legal issue. Public availability of information also negates the requirement for consent. Given the current proliferation of all types of information on the Internet, this condition opens the question of "What is publicly available personal information and how will this definition affected by use of the Internet?"

If collection and use or change of use is in the best interest of the individual, consent is not required. Collection of information for journalistic or artistic/literary endeavors also does not require knowledge on the part of the individual the information is about. Collected information may be used for additional purposes or disclosed to other than originally intended parties without consent to deal with an emergency which threatens the individual. Change in use or disclosure also applies to information that has been collected for academic research or statistical purposes without consent, however, the Privacy Commissioner must be notified prior to the use or disclosure or the information.

Disclosure without consent is allowed under Bill C-6 in numerous circumstances, many related to the legal actions of the collecting organization. The first two, and most likely most used, among these is the disclosure of personal information to legal counsel which has been retained by the organization and release of information to a third party for collection of a debt owed to the organization. Third, consent is not required for the release of information when the disclosure is required for compliance with a court order or a request from any other legal body in the course of enforcing or investigation of a violation of federal or provincial laws. Unrelated to the legal activities or obligations of an organization, personal information can be disclosed once one hundred years have passed since creation of the record of information or twenty years after the death of the individual the information was about. One final allowable instance of disclosure without consent is for archival purposes.

Limited Collection: In order to ensure compliance with the intentions of Bill C-6 to protect the privacy of Canadians, collection of information should be limited to only required information. This assists organizations with compliance with Bill C-6 by reducing the information that is being maintained by the organization. Also, this reduces the costs incurred by the organization for the initial information collection, information storage and the efforts required to maintain the accuracy and security of personal information.

Limited Use: Limiting the use, disclosure and retention of information will help to reduce the likelihood of a violation, similar the limitation on collection mentioned previously. Limiting the retention period will help to reduce improper use or disclosure, as information can not be used in any way if it no longer exists within the collecting organization's records or computer systems. This will also provide the benefit of reduced maintenance, storage and backup costs that must be incurred to retain information.

Accuracy: Reasonable efforts must be made by the collecting organization to ensure the accuracy of the information collected and retained. Increased accuracy helps organizations to reduce the risk of legal liability due to improper use or disclosure of inaccurate information. Documented procedures, based on the information security policy, will help to ensure that the information gathered is accurate at the time of collection and any necessary steps are performed to validate retained information on a periodic basis. One step which can be taken to assist with these efforts is to record the name, contact information, consented use and disclosure and the date the information was collected.

Safeguards: Information which has been collected and retained must be protected against theft, inadvertent disclosure and unauthorized access, copying, use or modification. This can be accomplished through a combination of controls including, but not limited to, implementation and enforcement of policy developed specifically for personal information, physical security at the storage location(s) and logical access controls such as passwords or encryption. One aspect of a sound information security policy that greatly increases the safeguarding of personal information is only allowing the minimum access required for any individual or party to perform their duties.

Openness: Once an information security policy has been developed, approved and implemented, all customers, clients and employees should be notified and given the location of security policy. To help ensure that the information security policy is openly available to everyone dealing with an organization, the policy and associated procedures and practices should be clearly written and easily understood. Not only must the policy be accessible, the name and contact information for the individual accountable for the protection of personal information and the information necessary to file access requests and the steps to be taken to file a complaint regarding the handling of personal information. One additional group of information which must be readily available is the types of personal information disclosed to subsidiaries or third parties and the reason for this disclosure. Having this information available about collected personal information allows individuals to ensure their information is being handled properly. Also, employees should be educated in the appropriate handling protection measures to be followed when dealing with personal information to improve an organizations overall compliance with Bill C-6.

Access: The principle of access is addresses the individual's rights to gain access and request modifications to data which has been collected. Upon request Bill C-6 requires

organizations to inform individuals if information is possessed and explain intended usage and/or organizations with which the information has been shared. Secondly, access to information which has been collected must be granted and corrections made to personal information which is inaccurate. Once inaccurate information is discovered, the organization is required to inform all parties with whom the information has been shared that the personal information is inaccurate or erroneous. At the individual's request, organizations are also required to provide a copy of collected information or the reason that access is not being granted. Once a request for access has been received, an organization must respond to the request within thirty days or be in violation of Bill C-6. There should be only a minimal charge, if any, for gaining access to personal information, and if a charge is to be incurred, notification must be given prior to processing the request. The information provided to any person must be easily understood and not reveal information of another individual.

Subsection 8(4) of Bill C-6 allows for an additional thirty days to respond to a request given certain circumstances. These circumstances include unreasonable interference with daily operations of the organization, additional time requirements for consultations or time requirements necessary to convert the information from its current form to one which is easily understood by the individual and does not reveal any personal information of another person. If this allowance is to be exercised, the requestor must be notified of the extension and also of their right to file a complaint with the Privacy Commissioner.

Similar to the principle of consent, access to information can be denied to any individual, providing the circumstances fall within the guidelines of Section 9 of Bill C-6. Two distinct groups of access denial are outlined as mandatory and discretionary. In the event providing access to personal information to an individual will reveal information about another individual, the organization must refuse to grant access, provided that the requested information can not be separated any other information. The second mandated refusal of access to information occurs when the information has been disclosed to a government body for the purpose of law enforcement and the government body has instructed the organization not to allow access to the information. The Privacy Commissioner must be notified whenever a request is received for such information. In the process of denying access to the individual, the organization is restricted to informing the individual only that access has been denied, but not that the refusal is at the request of a government body or that the Privacy Commissioner has been notified.

Five situations are detailed in which the right of refusal is left to the discretion of the organization which has collected the information. First, allowing access to personal information which will reveal confidential company information that can not be removed has been determined to be a question best answered by the organization. In the event allowing access to personal information will create a situation that could result in harm to another individual or threaten their security, the organization has the right to deny access to information, however, the individual must be notified of the reason(s). Access may also be readily refused if the information is protected by lawyer-client privilege or the

information itself was created during the proceedings of a formal dispute resolution. Due to the nature of the information which is covered by Bill C-6, other types of legal privilege, such as doctor patient privilege, do not apply. Finally, if the information was collected without the individual's knowledge or consent and the information was required to investigate either a breach of contract or violation of a federal or provincial law, as outlined previously, access may not be granted, however the Privacy Commissioner must be notified.

Recourse: As part of the development of procedures and practices for the protection of personal information, a simple complaint handling procedure should be developed. One of the largest benefits of such a procedure is that the way in which complaints are dealt with reflect on the general public perception and confidence in the organization. As part of the complaint procedure, the individual filing the complaint should be notified of additional avenues of recourse. These additional methods of recourse include industry associations, the Privacy Commissioner and regulatory bodies with jurisdiction over the organization. To ensure consistent action when a complaint is received, all complaints should be investigated and appropriate action taken. In order to handle complaints in a timely and complete manner, complaints should be acknowledged and the date and nature of each complaint recorded. This will also provide a detailed record in the event a complaint is escalated beyond the organization. Given the requirements of Bill C-6 in the area of complaint investigation and handling, a number of individuals must be on staff with the required skills, access to records and employees and authority to investigate complaints regarding personal information. Once complete, the individual should be notified that the investigation has been completed and all actions taken as a result. Whenever applicable, policies/procedures/practices or personal information should be modified based on the findings of the investigation. There is no time limit for filing a complaint unless the complaint relates to a refusal to grant access to information. In this situation, the individual has six months to file the complaint with the organization.

Impact

The impacts that these principles have on information security not clearly defined within the principle themselves are as varied as the principles themselves. The broadest and most far reaching effect is the legal requirement for the development and implementation of an information security policy and associated procedures and practices. For those organizations which do not already have a computer security program in effect, this provides a starting point for designing and implementing such a program.

As part of the implementation program for an information security policy, system infrastructure should also be analyzed to ensure that the components themselves assist in the protection of information. This may prove most beneficial in a situation where information security is viewed as a cost with no discernible benefit. The legal requirements of Bill C-6 can provide the needed emphasis on security throughout the organization to allow for capital spending allocations to the computer and network

infrastructure.

Also, providing open access to the personal information which is collected during the normal course of business operations will demonstrate to customers, partners and the public in general that the organization is performing at an expected moral and ethical level. This will help to engender confidence in the organization, providing potential economic benefit as a result.

Bill C-6 introduces new offences to the Criminal Code, related specifically to the mishandling of personal information. The offences are obstruction of the Privacy Commissioner during an investigation, destruction of personal information records and the dismissal or reprimand of an employee for reporting violations of Bill C-6, so called "whistle-blowing". These offences are punishable by a fine of up to $10,000 for a summary conviction or $100,000 for an indictable conviction[4].

The authority of the Office of the Privacy Commissioner is expanded by Bill C-6. The Privacy Commissioner is now able to initiate investigations into potential non-compliance and audits of organizational policies and practices in the area of personal information management and protection to ensure compliance. In the event of a complaint being filed with the Privacy Commissioner, the office has the authority to act as a mediator between the involved parties to resolve the issue. If a resolution can not be reached, the Privacy Commissioner can escalate the issue to the Federal Court within forty-five days of issuance of the resolution report. This escalation can be initiated by either the Privacy Commissioner or one of the parties involved. As an additional means of enforcing Bill C-6, the Privacy Commissioner may publish any management practices of an organization, if deemed to be in the best interest of the public. Also, the Privacy Commissioner is required to submit a report to Parliament at the end of every year detailing his/her activities over the year, including introduction of substantially similar legislation by the provinces. To promote knowledge of and compliance with Bill C-6, the Privacy Commissioner

At present, numerous computer security guidelines, standards and models which can be applied or followed, including the ISO/IEC models, CobiT, the Common Criteria for IT Security Evaluation and others. Each of these has its own area of focus, but are only suggested methods of establishing secure computing environments. Bill C-6 establishes a legal mandate requiring a specified level of information security, which can voluntarily be applied to all information maintained by an organization, not just personal information that is collected for commercial purposes.

The European Union passed The European Directive 95/46/EC in 1995. This directive contains standards pertaining to the use, protection and disclosure of personal information. The directives were required to be implemented by member nations by

---

[4] Bill C-6. April 13, 2000. URL: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html. (January 30, 2002)

October 1998. One basis of the directives is that personal information can not be shared with nations which do not provide protection of a similar nature. Bill C-6 has been determined to meet the requirements of the European Union, allowing such transfers to take place without implementation of further safeguards.

Conclusion

Bill C-6 represents a significant step forward in Canada for the protection of personal information. The conversion of the principles into a binding code of law establishes a minimum level of expected rights in the area of personal privacy and protection of personal information.

As most information is stored, processed and accessed with computer systems, this legislation is having extensive effects on all organizations which handle personal information. Creation of a legal obligation to develop and implement policies and practices to ensure protection of information and compliance with the individual principles results in a standard expectation from all organizations also provides a solid basis for the implementation of general security programs.

Bibliography

"Bill C6 – Canada". Internet Privacy Policies. URL: http://privatech.ca/htdocs/html/canada.cfm. (January 17, 2002).

Bill C-6. April 13, 2000. URL: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html. (January 17, 2002).

Brierly, Bill. Canada's New Privacy Act. April 5, 2001. URL: http://www.trm.ca/pages/t-tech4.html. (January 9, 2002).

"The CSA Code". Internet Privacy Policies. URL: http://privatech.ca/htdocs/html/the_csa_code.cfm. (January 17, 2002).

Manley, Honourable John. "Third Reading Speaking Notes Bill C-6." January 27, 2001. URL:http://www.ic.gc.ca/cmb/welcomeic.nsf/558d636590992942852564880052155b/85256779007b79ee8525681200667a45!OpenDocument. (January 31, 2002).

McMahon, Tamsin. Canadian privacy regulations meet EU standards. URL: http://europemedia.net/shownews.asp?ArticleID=7738. (January 18, 2002).

The Privacy Act. URL: http://privcom.gc.ca/legislation/02_17_01_e.asp. (January 9, 2002).

PrivaTalk – December 2001. URL: http://privatech.ca/htdocs/html/privatalk_sample.html. (January 17, 2002).

Your Privacy Responsibilities – Privacy Commissioner of Canada. URL: http://privcom.gc.ca/information/guide_e.asp. (January 1, 2002).

Your Privacy Responsibilities – A Guide for Canadians. URL: http://www.privcom.gc.ca/information/02_05_d_08_e.asp. (January 17, 2002).