Bill 207, *The Personal Information Protection and Identity Theft Prevention Act*

TARIQ MUINUDDIN

I. INTRODUCTION

Bill 207, *The Personal Information Protection and Identity Theft Prevention Act*[1] ("PIPITPA") was a private members' bill that was introduced in the fourth session of the 38rh Legislature of Manitoba. The purpose of the act was to create laws regulating the collection and use of personal information in a way that would make the province exempt from privacy regulation under the federal *Personal Information Protection and Electronic Documents Act*[2] ("PIPEDA"). PIPITPA did not make it to the committee stage and instead died on the order table.

This paper will begin by discussing the background events and relevant legislation leading up to the creation of PIPITPA. This section will give an accounting of the privacy laws already in place at the federal and provincial levels.

The next section of the paper will document the bill's progression through the legislative process. It will discuss the process that created the bill and the people who were involved. It will outline its history in the legislature from the first time it was introduced to current developments related to the bill.[3]

The final section of the paper will provide a substantive analysis of PIPITPA. It will explain what PIPITPA does. It will address the arguments for and against PIPTPA and show that PIPITPA is a good piece of legislation that would improve privacy protection in Manitoba.

Bill 207, *The Personal Information Protection and Identity Theft Prevention Act*, 4th. Sess., 38th Leg., Manitoba, 2005 [PIPITPA}.

S.C. 2005, c. 5 [PIPEDA}.

This paper was submitted November 2006. All information contained herein is current to that date, unless otherwise noted. An update is contained at the conclusion of the paper.

II. ORIGINS OF BILL 207

A. Background Information

In 1980, the Organization for Economic Co-Operation and Development ("OECD,) adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[4] Canada became a signatory to these guidelines in 1984.[5] The guidelines did not necessarily call for legislation, but rather set out principles that should be adhered to either by legislation or voluntary standards. This led to the creation of the Model Code by the Canadian Standards Association in 1996.[6] The Model Code set out 10 principles for privacy protection: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance.[7] The Model Code was created after extensive consultation with stakeholders, and it was further envisioned that industries would adapt the code to better fit their circumstances.[8]

In 1995, the European Union adopted Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data[9] {"the EU Directive"). This legislation set out policy that had to be in place for European organizations that collect, use or disclose personal information. This included policy regarding the transferring of this information outside the European Union. Organizations were forbidden from doing so unless the f:lreign country had suitable information protection.[10] would even apply to foreign branches of European companies. The EU Directive was to come into effect in 1998, and it was in response to this that the Canadian government enacted PIPEDA in 2000. PIPEDA is essentially a

---

OECD, *Guidelines on che Protection of Privacy and Transborder Flows of Personal Data, Preface,* online: OECD <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_l,OO.html>.

See *Englander v. TELUS Communications* Inc., 2004 FCA 387, [2005] 2 F.C.R. 572 at para. 12.

Canadian Standards Association, *Privacy Code,* online: Canadian Standards Association <http://www.csa.ca/standards/privacy/code/Default.asp?language=english>.

Ibid.

Ibid. at [11]introduction". For example, banks could agree upon their own variation of the Model Code, keeping in mind any statutory obligations they may already have, while video rental stores could agree on a less onerous one.

EC, *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* [1995] O.J. L. 281/31, online: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=celex:3199510046:en:html >.

10 *Ibid.* at s. 57.

codification of the principles and obligations set out in the Model Code, which is included as Schedule A of the act.[11]

PIPEDA came into effect on 1 January 2001 for organizations that collect, use or disclose personal information in connection with the operation of a federal work, undertaking or business, or for organizations that disclose this information outside their province.[12] These are two areas clearly within federal jurisdiction. A second date-1 January 2004-was set as the date when PIPEDA would come into effect for the remaining organizations unless the organization's province had enacted substantially similar legislation of its own.[13] Initially, only Quebec had legislation that satisfied PIPEDA's requirements-in fact, Quebec's legislation predates PIPEDA by seven years.[14] As the 1 January 2004 deadline approached, both Alberta and B.C. also enacted legislation that has subsequently been deemed substantially similar to PIPEDA by the federal privacy commissioner.[15]

B. Current Manitoba Legislation

Besides PIPEDA, the other relevant privacy legislation in Manitoba is the *Freedom of Information and Personal Privacy* Act[16] ("FIPPA"), the *Personal Health Information* Act[17] ("PHIA"), and the provincial *Privacy Act*.[18]

FIPPA governs how the provincial government can collect, use and disclose personal information.[19] This would include, for example, information related to a driver's license or student loan. The act also provides protection for public sector workers.[20] PHIA covers the use of personal information by health professionals, hospitals, and others who have access to health information.[21] The *Privacy Act* creates a tort of invasion of privacy. It protects against

---

11 See PIPEDA, *supra* note 2 at Sch. I. In contrast, the US government was able to negotiate with the EU so that American companies that did business with the EU only had to agree to a voluntary code. Perhaps showing a difference in relative bargaining power.

12 PIPITPA, *supra* note 1 at s. 72, proclaimed in force 1 January 2001, SI/2000-29, C. Gaz. 2000.11.914.

n See Office of the Privacy Commissioner of Canada, *Implementation Schedule*, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/legislation/02_06_02a_e.asp>.

14 *An Act respecting the protection of personal information in the private sector*, R.S.Q. c. P-39.1.

15 *See Personal Information Protection Act*, S.A. 2003, c. P-6.5 [PIPA] and *Personal Information Act*, S.B.C. 2003, c. 63.

16 S.M. 1997, c. *50*, C.C.S.M. c. F175.

17 S.M. 1997, c. 51, C.C.S.M. c. P33.5.

18 R.S.M. 1987, c. Pl25, C.C.S.M. c. P125.

19 *Supra* note 16 at s. 2.

20 *Ibid.*

21 *Supra* note 17 at s. 2.

activities like surveillance, spying, and following, as well as "the unauthorized use of someone's name, voice, likeness, or personal documents".[22] Most other provinces also have their own FIPPA, PHIA and *Privacy Act*.

III. BILL 207 IN THE HOUSE

A. The Political Motivation

Mavis Taillieu, the MLA for Morris, is the Progressive Conservative ('PC") critic for culture and tourism. As part of this portfolio, she is also the critic for matters relating to PIPPA. The idea for the proposed legislation came to her as part of this latter responsibility.[23]

Ms. Taillieu wanted to extend the benefits FIPPA gave to employees in the public sector on a provincial level to employees in the private sector. To her, the almost weekly reports of yet another company losing a laptop filled with personal information that shouldn't have been on a laptop in the first place are not the reason for the legislation. Rather, she said, they illustrate a situation that she believes the province should improve.[24]

Ms. Taillieu knew before she began working on PIPITPA that there was almost no chance of the government passing it.[25] Outside a minority government situation, private members' bills are rarely passed. Only five of the 38 private members' bills introduced during the previous sessions of this legislature became laws.

B. Drafting of the Legislation

Ms. Taillieu initially attempted to get the legislation drafted by the services available at the legislature. However, the people who were available to draft the bill did not have the grasp of privacy law she was looking for. Ms. Taillieu knew of Winnipeg business lawyer Brian Bowman because of his regular articles on privacy law in the *Winnipeg Free Press*. After meeting with Ms. Taillieu, Mr. Bowman provided his expertise and drafted the legislation, using Alberta's PIPA as a template and adapting it to fit Manitoba.[26]

---

12 Ian J. Turnbull, *Privacy in the Workplace: The Employment Perspective* (Toronto: CCH Canadian, 2004) at 107.

23 Interview of Mavis Taillieu by Tariq Muinuddin (23 November 2006) [Taillieu].

zi *Ibid*.

zs *Ibid*.

26 *Ibid.*

C. History in the Legislature

The bill was introduced as the *Personal Information Protection Act* in November 2004.[27] It had its second reading the following May. There was some debate about the bill, but because the government did not want to adopt the bill it was not referred to a committee.

Feeling that the issue was too important to ignore, Ms. Taillieu reintroduced the bill as the *Personal Information Protection and Identity Theft Prevention Act* in the fourth session of the 38th legislature. The duty to notify was added to the bill at this point, and its name was changed to reflect this. It was hoped that adding "Identity Theft Prevention" to the title of the bill would generate some interest in the public, thus increasing pressure on the government to consider the bill.[28] Again, there was some debate at the second reading, but the bill wasn't referred to a committee. The bill has been reintroduced in the current session of the legislature, but it does not appear that a different outcome will result.[29]

IV. ANALYSIS OF BILL 207

A. What Does PIPITPA do?

> The purpose of this Act is to govern the collecrion, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.[30]

Prior to PIPEDA, the only statutory protection afforded to Manitobans with respect to privacy was:

- For data collected, held and used by the provincial government (FIPPA) and federal government (through the federal *Privacy* Act[31]); and
- For health information handled by doctors, hospitals, the province, and potentially insurers (through PHIA).

Currently, organizations that are covered by the *Privacy Act* (such as federal government organizations) are not covered by PIPEDA.[32]

PIPITPA would extend privacy protection similar to that found in FIPPA or the federal *Privacy Act* to interaction with all organizations that use, collect or

---

27 BUl 200, *The Personal Information Protection Act*, 3«1 Sess., 38rh Leg.• Manitoba, 2005.

28 Taillieu, *supra* note 23.

29 Bill 200, *The Personal Information Protection and Identity Theft Prevention Act*, ,Sth Sess., 38ch Leg., Manitoba, 2006 was not enacted when the legislation session ended on 20 April 2007.

30 PIPITPA, *supra* note 1 at s. 3.

31 *Privacy* Act, R.S.C. 1985, c. p,21.

32 PIPEDA, *supra* note 2 at s. 4(2)(a).

disclose personal information for a commercial purpose in the province.[33] The act would also provide privacy protection to employees in Manitoba•s private sector. This would limit and control how employers in the private sector could use and collect their employees' personal infurmation.[34] Currently, there is no such protection. PIPITPA also would introduce a duty to notify affected people if an organization loses control of their information.[35] This second point is a novel feature for privacy legislation in Canada.

The cornerstone of this legislation is consent. Any organization that wishes to collect personal information must disclose its reasons for requesting this information. It must also specify how it will use the information.[36] The organization will then be able to use this information, but only for the uses that have been consented to.[37] When making a request, an organization cannot ask for consent to disclose more information than it requires.[38] If the organization wishes to use the information in an additional way at some later time it must obtain consent for this new use.[39] For the purposes of the legislation consent does not have to be explicit. Generally, providing the information requested will constitute consent.[40]

Information collected prior to the enacting of PIPITPA ais deemed to have been collected pursuant to consent given by that individuar'.[41] PIPEDA has no such clause and technically organizations would be required to dispose of any personal information that has not been collected in a PIPEDA compliant mannerY Under PIPITPA, organizations would be able to use this information for the purposes already consented to without having to ask for the consent again. However, if they wish to use the information for a new purpose they would have to get the consent of the person.[43]

---

33 PIPITPA, *supra* note 1 at ss. 3 and 4(1).

34 *Ibid.* at s. 3.

35 *Ibid.* at s. 34(2).

36 Ibid.ats.l3(1).

37 *Ibid.* at s. 8 (4).

38 Ibid.atss. 7(2) and 11(2).

39 *Ibid.* at s. 8 (4).

40 *Ibid.* at s. 8(2).

41 Ibid.ats.4(4)(a).

42 See Christopher S. Wilson & Jeffrey F. Vicq, "Exempting B.C. and Alberta: Stitching the Seamless Continuum" (2004) 1 Canadian Privacy Law Review 97 at 100: "PIPEDA contains no grandfathering provisions for information collected before it carne into force. Technically, organizations were required to destroy all personal information in their possession because arguably even the retention of the information without consent contravened PIPEDA."

43 *Ibid.*

Like PIPEDA, PIPITPA requires organizations to designate someone to ensure that the organization complies with the act. This person (or people) needs to have sufficient authority within the organization themselves, or they should have "sufficient official senior management support"[44] to ensure they will be listened to.[45] This requirement affects organizations large and small equally- even a comer video store would need a privacy officer.

Section 34(2) of PIPITPA places an obligation to notify on organizations that have personal information in their custody or control that is stolen, lost or accessed in an unauthorized manner. If such an event occurs, the organization is required to notify the people affected as soon as is reasonably practicable. Surprisingly, this is not an element of PIPEDA, or of the similar provincial acts.

B. Arguments in Favour ofPIPITPA

I. *Constitutionality of* PIPEDA

PIPEDA is a federal act. As such, there is some concern about its jurisdiction over matters which are purely of a provincial nature.[46] As large industry players already follow the Model Code, many practitioners had thought it highly unlikely that anyone would challenge the constitutionality of the act. The legal costs involved in bringing a case all the way to the Supreme Court, where it would likely be appealed to, would be prohibitive for smaller organizations. There is also the issue of economic harm should PIPEDA be ruled unconstitutional. Without the law in place, companies doing business in the EU would not be able to send any personal information to organizations in Canada. But in December 2003 the Government of Quebec initiated a challenge to the constitutionality of PIPEDA.[47] The case is still before the courts, with the province having submitted an affidavit in July 2006.[18] If Manitoba wants the protection that PIPEDA offers, it can do so by enacting substantially similar provincial legislation such as PIPITPA that would still protect Manitobans in the event of a successful constitutional challenge to PIPEDA. Furthermore, if

---

44 William Charnetski, Patrick Flaherty & Jeremy Robinson, *The Personal Information Protection and Documents Act: A Comprehensive Guide* (Aurora, Ont.: Canada Law Book, 2001) at 39.

45 Passing the responsibility to a person with little authority such as a mail clerk would likely not meet PIPITPA's requirements, unless it is made clear that the person can actually enforce compliance within the organization.

46 An example would be a local video store that records patron information, such as records of what movies they had rented.

47 See Simon Chester, "PIPEDA Reference Raises Vital Constitutional Questions" (2004) 1 Canadian Privacy Law Review 52 at 55.

48 Michael A. Geist, PIPEDA *Hearings-Day 01 (Industry Canada),* online: MichaelGeist.ca <http://www.michaelgeist.ca/content/view/1541/125>.

the other provinces of Canada enacted their own substantially similar legislation, most of the issues regarding PIPEDA's constitutionality would be rendered moot.

2. *Protection of employees in the private sector*

Currently, there is no legislation in place to protect the personal information of workers in the private sector. This means that organizations can collect data from their employees without consent. The organizations have no obligation to keep this information secure, and face no real consequences if it is accessed by someone who shouldn't access it. The current situation lets organizations collect far more information about their employees than they need, and provides no oversight for how this information is to be stored, used or disposed of.

An incident involving a McDonald's restaurant in Winnipeg is an example of what is possible.[49] In 2004, the restaurant started using palm scanners instead of punch cards to keep track of when employees got to work and left. McDonald's can keep these fingerprints for as long as it wants. It can pass them along to its business partners--or the Department of Homeland Security. The organization does not have to inform affected employees if unauthorized access to this information has occurred. As a result, a McDonald's personnel file contains a person's name, address, social insurance number and fingerprints-a goldmine for identity theft, which arose because McDonald's wanted to keep track of its employees' hours.

There is nothing in PIPEDA that will provide protection in this situation, so it is up to the Province of Manitoba to resolve this issue. The Manitoba Federation of Labour is one organization that wants this protection,[50] and it speaks for the very people affected. Passing PIPITPA would be one way of doing this.

3. *Enforcement*

Under PIPEDA, the dispute resolution process is as follows:[51]

- An individual[52] makes a complaint to the Privacy Commissioner in Ottawa;

---

49 Graeme Smith, "Is Big McBrother invading workplace privacy?" *The Globe* and *Mail* (13 January 2004).

50 Taillieu, *supra* note 23.

51 Turnbull, *supra* note 22 at 85.

52 There is no requirement that the individual be directly affected by the act complained of. See H. H. McNairn & Alexander K. Scott, A *Guide to the Personal Infonnation Protection and Electronic Documents Act*, 2006 ed. (Markham, Ont.: LexisNexis Canada, 2006) at 55.

- The Commissioner gives a nonbinding recommendation after investigating the matter;
- If one of the parties is unhappy with the result, it can appeal to the Federal Court (which would be in Winnipeg for parties in Manitoba). Similarly, if the organization doesn't follow the Privacy Commissioner's recommendation, the complainant can apply to the Federal Court for a hearing on the matter; and
- From this point on the regular ttial process is followed.

PIPEDA is primarily enforced by the individuals who make complaints.[53] Making complaints to the Privacy Commissioner is a relatively straightforward and inexpensive process. But once proceedings move to the courts, the expense becomes out of reach for most people. In both Alberta and B.C., the provincial Privacy Commissioners have order making powers-their decisions must be followed.[54]

As it was proposed, PIPITPA would not be able to create a provincial office of Privacy Commissioner, or give it order making powers. But this is only because of the legislative limitations of private members' bills-they cannot have any provisions for penalties. If the government wished, it could fix the legislation, or introduce a stronger version of its own that would create a provincial Privacy Commissioner with the power to make binding decisions with respect to complaints. Under a "Hxed" PIPITPA, any appeal of the Privacy Commissioner's orders would be heard in the Court of Queen's Bench.[55] This means those living outside the Winnipeg area wouldn't have to travel as far to get to court.

4. The duty to notify

PIPITPA's duty to notify provisions are an important tool to prevent identity theft.[56] It is almost common news to hear of laptops with sensitive information being stolen, and such breaches can have a significant effect on the people whose information has been taken. Requiring organizations to notify the people who are potentially affected by such breaches forces them to take precautions and increase their vigilance with respect to identity theft. It also places the organization in a position where it has to go before the people affected and explain how their personal information was compromised. This speaks directly

---

53 The Privacy Commissioner has the power to initiate a complaint of its own motion. See *ibid.* at *56*.

54 Christopher S. Wilson, *supra* note 42 at 101.

55 Actions commenced under PIPITPA would be heard in Manitoba's Court of Queen's Bench, which sits throughout the province. PIPEDA actions, however, are heard in Federal Court, which only sits in Winnipeg and is thus less accessible to litigants.

56 PIPITPA *supra* note 1 at s. 34(2).

to the principle of accountability in the Model Code. Absent such a duty, it would be up to individuals to check up on all the organizations that have their personal information to make sure that it is still indeed safe.

5. Parliamentary review

PIPEDA includes provisions for its review every five years by a committee of Parliament. These reviews provide an opportunity to make changes, such as including a duty to notify. Parliament need not wait until a review period to make this change, however. But, since the other provinces do not currently have this duty, it is doubtful there is enough will for it to be mandated across the country. It is unlikely that Manitoba's privacy concerns would be enough to get Parliament-which is dominated by Ontario and Quebec-to listen. PIPITPA would allow Manitobans to address these concerns without worrying about what the other provinces want to do. PIPITPA also includes its own provisions for review to make sure that stakeholders can voice their concerns with the legislation. It would come up for review 18 months after being enacted and then at least every three years after that.[57]

6. *Centralization of privacy law*

The provincial government has started to introduce amendments to existing legislation to increase privacy protection in Manitoba. While this is a positive first step, there is a compelling argument to be made for having a "visible, broadly applicable statute".[58] One element of this argument would be efficiency. Instead of having to parcel out added roles and responsibilities to regulators that were outside of their core competencies, having one office (that of the Privacy Commissioner) working on privacy issues would allow expertise in the area to be consolidated and used more effectively. One uniform statute would also increase the clarity of the law. Stakeholders would know that they only had to look at one statute, and only had to contact one office to deal with privacy issues. This makes it easier for organizations to comply with the law because it would be accessed at a single location. The proposal also makes it easier for individuals to learn about and act on their rights, because it reduces the amount of searching they have to do.

Having only one piece of legislation would also increase the visibility of the law. According to Ms. Taillieu, who brought PIPITPA forward, many stakeholders haven't heard of PIPEDA, or only vaguely know of its scope and effect.[59] By

---

57 *Ibid.* at s. 43(1).

58 Bryan Schwartz & Darla Rettie, "Bridging the Privacy Gap: The Case for Enacting Substantially Similar Privacy Legislation" (Paper presented to the 2004 Isaac Pitblado Lectures, 19 November 2004) *Privacy--Another Snail in the Ginger Beer,* (Winnipeg: Law Society of Manitoba, 2004) at 5.

59 Taillieu, *supra* note 23.

creating a new privacy law, the province would send a strong message to Manitoba stakeholders that privacy is an issue it takes seriously.

7. *Privacy legislation in other provinces*

Currently, Quebec, Alberta and B.C.[60] have their own provincial legislation which is substantially similar to PIPEDA. As their laws were created after PIPEDA, Alberta's and B.C.'s politicians must have had good reasons for wanting to have their own privacy legislation instead of PIPEDA. Excepting the duty to notify, all the advantages PIPITPA has over PIPEDA are present in Alberta and B.C's privacy legislation. This makes sense, because PIPITPA is based on Alberta's PIPA.[61]

The reasons for PIPITPA that have been described in this section and the previous one are not the only ones considered by the provinces. Alberta's PIPA was designed to be easier for small businesses to comply with. Also, it only affects not for profit and charitable organizations if they are carrying out commercial activities.[62] In the debate during the second reading of PIPITPA, Nancy Allan, the Minister of Labour, stated that no other province was developing private sector privacy legislation[63] and used this as another reason to hold off on passing Bil1207. This was a strange thing for her to say, considering PIPITPA was based on similar Alberta and B.C. legislation that covers the private sector.

C. Arguments Against PIPITPA

1. The *bill isn't substantially similar* to PIPEDA

One set of arguments against PIPITPA focuses on duplication between federal and provincial privacy legislation. Provincial legislation that is not substantially similar to PIPEDA would create a situation where Manitoba organizations would have to comply with two sets of regulations. It is thus highly desirable to create provincial legislation that is deemed to be substantially similar to PIPEDA. Otherwise, the government has noted, unnecessary duplication, costs and confusion would result.[64]

---

60 See *supra* note 14 (Quebec legislation) and *supra* note 15 (Alberta and B.C. legislation}. In fact, legislators from Alberta and B.C. worked together in drafting their legislations: Colonel Michel W. Drapeau & Marc -Aurele Racicot, *Protection of Privacy in the Canadian Private and Health Sectors* (Toronto: Thomron Canada, 2006} at AB-1.

61 Brian Bowman, "NDP should support privacy bill or say why not" *Winnipeg Free* Press (1 March 2006}.

62 Drapeau, *supra* note *59* at AB-1.

63 Manitoba, Legislative Assembly, *Debates and Proceedings*, Vol. LVII No. 72A (18 May 2006) at 2274 (Nancy Allan).

64 *Ibid.* at 2271 (Greg Selinger).

To be substantially similar, legislation must:

- Incorporate the 10 principles in Schedule 1 of PIPEDA;
- Provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- Restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.[65]

This bill is a private members' bill. As such, it cannot contain any penalty provisions. Contrast this with PIPEDA, whose penalties include a maximum of $100 000 in fines.[66] As a result, any legislation that sought to be substantially similar should have penalties as well. The legislation's absence of penalties means it would not be deemed substantially similar to PIPEDA, resulting in duplicate legislation.

Similarly, to be substantially similar, PIPITPA would have to have its own oversight and investigatory mechanism. These features cannot be included in a private members' bill.[67]

However, as previously discussed in the section on enforcement, this is something the government would be able to fix if it decided to go this route.

2. *Education*

The government also stated it felt it was more important to focus on education about identity theft so people and organizations could be more aware of the risks and responsibilities that they face.[68]

To that effect, it had created websites featuring educational kits that allow both individuals and companies to learn how they can combat identity theft.[69] However, there is nothing preventing the government from focussing on education while also introducing a new law that dealt specifically with identity theft and personal information. It could even be argued that a new law would increase the motivation for stakeholders to make use of the educational materials prepared by the government as they would have a practical reason for doing so. The education and legislation would complement and reinforce each other.

3. *Cross-border information*

One significant issue with any provincial law like PIPITPA is that it would not have jurisdiction over information that crosses a border. Many companies would

---

65 Schwartz, *supra* note 57 at 1.

66 PIPEDA, *supra* note 2 at s. 28(b).

67 *Supra* note 62 at 2272 (Greg Selinger).

68 *Ibid.* at 2271.

69 *Ibid.*

be subject to both pieces of legislation even if PIPITPA was deemed substantially similar to federal legislation because they do business in the United States, other provinces or other countries. Forcing these companies to deal with two sets of regulations-even if the provincial legislation is similar to the federal one--decreases the utility of the provincial legislation. This is what currently happens in Alberta:

> Thus, it is possible that where the collection of information occurred in Alberta but the organization subsequently discloses such information outside of Alberta, PIPA would govern the collection activity and PIPEDA would govern the subsequent disclosure activity. This is consistent with an activities-based view on the regulation of privacy.[70]

Organizations would have one set of laws for the collection and use of the data within Manitoba, and another for its use outside the province. This cannot be avoided. It may be mitigated, however, by the fact that being compliant with PIPITPA will usually make an organization compliant with PIPEDA as well. If the organization applied the standard of care needed for the provincial legislation, it would also meet PIPEDA,s requirements.

4. Cost to the province

The cost associated with enforcing the act is another aspect that may have been in the mind of the government. If the bill was passed, the province would have to create and fund· its enforcement and investigatory mechanism. However, the province may be able to save money by having the cases go to Federal Court. By having only the federal act, the provincial government will be able to offload the costs associated with it. This was pointed out by Cliff Cullen, the MLA for Turtle Mountain who said during the second reading of the bill: "It is not a matter of passing the buck, and I know this government likes to pass the buck and rely on the federal government to do their work for them".[71] The government will have to decide if the cost of creating a Privacy Commissioner and enforcing the law is worth the benefits arising from PIPITPA.[72]

5. Consultation with stakeholders

The government also raised the issue of inadequate consultation-in its mind, Ms. TaUlieu did not engage in enough consultation with stakeholders to see if there was public support for the bill.[73]

---

70 Stephen D. Bums, "2004: Alberta's First Year of Private Sector Privacy" (2005) 2 Canadian Privacy Law Review 68 at 69.

71 *Supra* note 62 at 2277 (Cliff Cullen).

72 Ontario's Information and Privacy Commissioner's budget for 2006-2007 is an estimated $12 132 800. See Information and Privacy Commissioner of Ontario, *2006 Annual Report* (Toronto: Information and Privacy Commissioner of Ontario) at 60.

73 *Supra* note 62 at 2274 (Nancy Allan).

Ms. Taillieu did engage in consultation, but she found that most stakeholders didn't know enough about the issue to make any contribution. Nationally, there is very little awareness of or compliance with PIPEDA. In her article "The PIPEDA Five Year Review: An Opportunity to be Grasped", Philippa Lawson wrote extensively on the lack of compliance with, and awareness of, PIPEDA. On compliance, she said that "few studies of business compliance with PIPEDA appear to have been conducted, or at least made public. The only significant study is shrouded in mystery."[74] Speaking to that study, Lawson said it:

> Found that "only a small number of businesses have established clear and specific processes for the collection, use and disclosure of personal information", and that [11]most companies have ... written weak, vague policies that serve only to try to appease customers", despite their obligations under PIPEDA.[75]

Moreover, Lawson said, this study does not appear to be publicly available. She also cited two other limited PIPEDA compliance studies, one of which described "... continuing problems with these corporations' use of 'implied consent' obtained by 'opt out' mechanisms". The other study, meanwhile, concluded that business "implementation of the PIPED Act has been ad hoc at best and non existent at worst".[76]

On the subject of awareness, Lawson referred to a recent poll commissioned by the Privacy Commissioner. The poll found Canadians are generally in the dark about the country's privacy law. Most strikingly, over half of those who were surveyed were unaware of "any laws that help Canadians deal with privacy and the protection of personal information".[77] Commenting on the findings, Lawson said:

> This information deficit no doubt explains in part why more complaints are not forthcoming, and seriously undermines the effectiveness of a complaints-based enforcement regime. Either public awareness needs to be drastically improved, or the approach to enforcement under PIPEDA needs to be altered so as not to rely so heavily on individual complaints.[78]

The studies support Ms. Taillieu's assertion that stakeholders do not know enough to make consultation anything more than an exercise in education. She also argues that government doesn't always have to react to events but can- and should-be proactive in situations where it sees the need for a law.[79] This might require action against serious stakeholder opposition, such as in the case

---

74 Philippa Lawson, "The PIPEDA Five-Year Review: An Opportunity to be Grasped" (2005) 2 Canadian Privacy Law Review 111 at 111.

75 *Ibid.*

76 *Ibid.*

77 *Ibid.* at 112.

78 *Ibid.*

19 Taillieu, *supra* note 23.

of seatbelt laws which were almost universally rejected by stakeholders but were passed regardless of that opposition. Presently, it is only after something bad happens to them, such as having their identity stolen, that people begin to think about privacy issues and laws. If the province waits for enough people to learn about privacy protection the hard way, it will already be too late.

6. *Vnifonnity of laws*

The government also generally favours one set of legislation across the country. It feels that one law would provide greater uniformity across the country and reduce the cost of doing business across the country. [80] There are two rebuttals to this.

The first is that even if there were 13 laws across the country, it would not be hard for organizations to adopt procedures that simultaneously comply with the requirements of all jurisdictions because the laws would be substantially similar. This is especially true because the laws are all supposed to be based on the Model Code.[81]

The second rebuttal is that in many cases the provincial laws are actually more business friendly. Alberta's PIPA has been hailed by businesses as being superior to PIPEDA.[82] So it is quite possible that businesses would find it advantageous to work under a scheme where the provinces have their own legislation that is both substantially similar to PIPEDA and better for business as well.

7. *Technological advances*

The government also seems to have a desire to combat identity theft through the use of smart cards. But at the same time, it also points out that smart card technology is still a ways from being as robust and secure as it would like. Jim Maloway, the MLA for Elmwood, gavthe example of Ontario's Harris government's plan to implement smart cards following the lead of banks.[83] But after a few years and a lot of money, the government concluded the technology wasn't quite ready. The banks still haven't moved to smart cards, and in fact find it cheaper to pay out losses whenever identity theft happens instead of trying to stop the problem with smart cards. [84] He suggested the province should wait until the banks have developed a secure smart card technology (in effect offl.oading the costs to the banks) before it moves in that direction.[85] In the

---

80 *Supra* note 62 at 2277 Qim Maloway).

61 See PIPITPA, *supra* note 1 at Sch. I, which is a codification of the Model Code.

92 Bowman, *supra* note 61.

83 *Supra* note 62 at 2278 Qim Maloway).

84 *Ibid.*

85 *Ibid.*

meantime, he said the government should educate people and encourage them to use paper shredders.

Any discussion of smart cards invariably includes the use of Radio.-Frequency Identification (uRFID") tags. Advances in RFID have resulted in tremendous improvements in their storage capacity, and reductions in their cost and size. Presently, researchers have developed "smart dust" that is so small it is invisible to the human eye.[86] The U.K. government already has RFID.-enabled smart identity cards, so there is no need for the government to wait for the banks- the technology is good enough right now. The security of the U.K. smart cards has also already been compromised.[87] It is a fact of life that moments after a better safe is built, someone will find a way to open it. There is never going to be a point where smart card technology will be perfectly secured. If the government is serious about implementing them, there is no pressing technological reason barring their introduction.

B. Credit

The opposition raised responsibility for the bill as another reason why the government was opposed to Bill 207.[88] If the government made the amendments necessary to make the bill work, Ms. Taillieu and the PC party would receive most of the credit for the bill. On the other hand, if the government rejects the bill, but then introduces a similar bill at a later time, it would be able to get credit for the effort put in by Ms. Taillieu. Another, slightly less obvious way for the government to get credit for the bill would be to amend existing bills to include privacy provisions. This would allow the government to claim it had changed a number of laws to better protect the privacy of Manitobans. This session, for example, the government introduced BillS, *The Personal Investigations Amendment Act.*[89] This act will add protective mechanisms for people who suspect they may be the victim of identity theft.[90]

9. PIPEDA's *review process*

PIPEDA comes up for review this year. The government believes it can make its voice heard during the review process and have any of its concerns dealt with at

---

86 Ann Cavoukian, nTag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology" {2004) 1 Canadian Privacy Law Review 76 at 76.

87 Steve Boggan, "Cracked it!" *The Guardian* (17 November 2006), online: Guardian Unlimited <http://www.guardian.co.uk/idcards/story/01950226,0t1html >. ',

88 Manitoba, Legislative Assembly, *Debates and Proceedings,* Vol. LVI No. 53A (25 May 2006) at 2990 (Kevin Lamoureux).

89 5th Sess., 38th Manitoba, 2006 (assented to 7 December 2006), S.M. 2006, c. 28.

90 *Ibid.* at s. 12.1.

that time.[91] The review process is ongoing at the time of this paper, thus the potential changes to PIPEDA are not yet known.

D. The Bottom Line on PIPITPA

PIPITPA has too many benefits to keep it from being eventually enacted.[92] It replaces PIPEDA with a law that is dearer, better for business, better for employees, and better for the privacy of Manitobans. The arguments for it are compelling and reasoned. The arguments against it sound more like the excuses of a government that was caught flat footed by the bill and is trying to buy time as it figures out what to do than bona fide criticism.

It is likely Ms. Taillieu's efforts have not gone unnoticed. *The Personal Investigations Amendment Act* will allow people to place a security alert on their credit report if they feel someone may be trying to use their identity to apply for credit.[93] The identity of the person using the credit must be verified if a security alert is present on a credit report. It is possible the government will try to introduce other amendments that will have the same effect as PIPITPA would have.

V. CONCLUSION

PIPITPA represents a very good political move by Ms. Taillieu and the PC party. They put the government under pressure by introducing and reintroducing the bill each session. In the highly improbable event the government passed the bill, a great deal of political credit would go to the PCs. If the government were to flat out vote against the bill-instead of simply not voting on it as it has done twice already-it would be on record as being against the bill and policy that most stakeholders in the province would view as desirable. During debate on PIPA (the original incarnation of PIPITPA), Mr. Kevin Lamoureux, the MLA for Inkster, wanted the government to vote on the bill so its position would be on record.[94]

If it continues its waiting, the government will be seen as doing nothing on an issue that is becoming increasingly important both provincially and nationally. Furthermore, Ms. Taillieu's reintroduction of the bill at each session has forced government to give reasons for failing to pass the bilL These statements, recorded in Hansard, could be used against it either during an election campaign or in the event of a high profile breach of privacy.

---

91 *Supra* note 62 at 2272 (Greg Selinger).

92 If not PIPITPA itself, some other substantially similar legislation should be enacted.

!H *Supra* note 88 at s. 12.1.

94 *Supra* note 87 at 2989 (Kevin Lamoureux).

VI. Update

A. The Current Status of PIPITPA

As previously noted, PIPITPA was reintroduced in the fifth session of the 38th Legislature. In that session the bill only had a first reading and there was no further debate on it. PIPITPA has been re..introduced once again in the first session of the new Legislature, but again there is very little chance of it being enacted.[95]

B. The PIPEDA Review Process

The federal Standing Committee on Access to Information, Privacy and Ethics held hearings on PIPEDA between 20 November 2006 and 22 February 2007. Its report was presented to Parliament on 2 May 2007. Of the 25 recommendations made in the report, the final three related to a duty to notify. From the report:

> Recommendation 23
>
> The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.
>
> Recommendation 24
>
> The Committee recommends that upon notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.
>
> Recommendation 25
>
> The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consene' power to notify credit bureaus in order to help protect consumers from identity theft and fraud.[96]

At present, there has been no government response to the report. However, it seems likely many of the recommendations will at some point be implemented because there is majority support for them. While the adoption of such provisions into PIPEDA would reduce some of the benefits of PIPITPA, it would still be beneficial for Manitoba to enact PIPITPA or similar legislation. The committee itself noted that much of the PIPEDA review process is aimed

---

95 Bill 206, *The Personal Infonnation Protection and Identity Theft Prevention Act,* 1st Sess., 39'h Leg., Manitoba, 2007.

96 Parliament, Standing Committee on Access to Information, Privacy and Ethics, "Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)" *inHouse of Commons Debates,* No. 145 (2 May 2007) at 1520 (Hon. Torn Wappel).

at "fine,tuning" PIPEDA to harmonize it with substantially similar provincial legislation. That reference should be made to the Alberta and B.C. laws, because they are "second generation" laws that have had the benefit of drawing upon the experiences of the Quebec and the federal acts. According to the committee, they "provide a more practical and updated reflection of privacy protection today."[97] By enacting its own legislation, Manitoba would get a louder voice in the next review process in addition to the benefits that such an act would give Manitobans.

97 *Ibid.* at 1.