

March 5, 2009

Honourable D. Toth
Speaker of the Legislative Assembly
Room 129 Legislative Building
2405 Legislative Drive
REGINA, SK S4S 0B3

Dear Mr. Speaker:

Re: *The Traffic Safety Amendment Act, 2008 (Bill 72)*

I write today to offer commentary on Bill 72, *The Traffic Safety Amendment Act, 2008*. I request that this be tabled in the Legislative Assembly pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act*. That section provides as follows:

33 The commissioner may:

(a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs; . . .

The purpose in providing this commentary is to provide the Assembly with our assessment of the impact this Bill may have on the privacy rights and protection of Saskatchewan residents.

Bill 72 has two main elements. One element deals with the treatment of vehicles operated by volunteer firefighters and first responders¹. The second element enables three different kinds of identity documents:

- (a) a two piece driver's licence including both a licence certificate and a photo identification card;
- (b) an enhanced driver's licence that is a single document; and
- (c) an enhanced photo identification card. This submission deals only with the second element in Bill 72 and more particularly the enhanced driver's licence and the enhanced photo identification card.

/2

¹ Section 10.

Saskatchewan Government Insurance (SGI) advises that the purpose of these two new identity documents is to satisfy the requirements of the United States Western Hemisphere Travel Initiative (WHTI). This instrument requires all travelers, including Canadian citizens, to present a passport or other approved secure document when entering the U.S. The WHTI is a response to security concerns regarding the events of 9/11. The WHTI is a result of a requirement in the U.S. *Intelligence Reform and Terrorism Prevention Act of 2004*. It directs the Department of Homeland Security (DHS) to devise a plan for additional safeguards relating to border identification requirements. Effective June 1, 2009, Canadians will need to present a passport at U.S. land and sea ports of entry, or a passport alternative that is acceptable to DHS.

I recognize the interest in collaboration with the United States federal government as well as states bordering Canada to improve security at our shared international border. I also understand the convenience of creating an identity card for those residents who do not hold a driver's licence. I am certainly not opposed to the commitment to introduce an alternative border crossing document to the Canadian passport. I do however want to make sure that reasonable privacy protection is incorporated into the design of that alternative document.

I attach a list of resource materials that my office has found useful for our consideration of Bill 72.

BACKGROUND

This office was advised by Saskatchewan Government Insurance (SGI) in June of 2008 that it was proceeding to develop an enhanced driver's licence (EDL) to meet the requirements of the Western Hemisphere Travel Initiative (WHTI). This was being done to parallel developments anticipated in British Columbia, Ontario and other Canadian provinces. We were advised that the plan was to be able to issue the enhanced driver's licence and the enhanced photo identification card by June 1, 2009.

We anticipate that the EDL will include the following elements or data fields:

- Name
- Address
- Birth Date
- Driver Licence Number
- Driver Licence Class

(Continued on next page)

- Issue and Expiry Dates
- Entitled Holder Signature
- Picture of Entitled Holder
- Height, Weight, Eye Colour, Hair Colour, Gender
- Embedded radio frequency identification (RFID) tag or chip
- Canadian Flag
- Restriction and Endorsement Codes
- Magnetic Stripe
- Unique number/stock serialization
- MRZ – border facilitation technology

We anticipate that the enhanced photo identification card would include the above features except for the driver licence number, driver licence class and perhaps restriction and endorsement codes.

We requested and were assured that a formal and comprehensive Privacy Impact Assessment (PIA) would be undertaken by SGI and then provided to us in a timely way. The PIA is a tool available at our website, www.oipc.sk.ca. It requires that a government institution carefully consider the authority for any new policy or legislative initiative that will impact the privacy rights of Saskatchewan residents. It poses a number of questions and considerations that the government would need to answer in order to determine whether the particular initiative is consistent with the applicable privacy law as well as policy and best practices. A PIA is commonly used in Canada to ensure that new policy or program initiatives of any public body fully comply with the applicable privacy laws and best practices.

We advised SGI that once we reviewed the PIA we would provide our advice to SGI and to the Legislative Assembly with respect to the privacy considerations generated by the enhanced driver's licence proposal. We indicated to SGI that our report would be an assessment of the extent to which this initiative complies with *The Freedom of Information and Protection of Privacy Act*² (FOIP), *The Health Information Protection Act*³ (HIPA), the *Overarching Privacy Framework for Executive Government*⁴ (the Privacy Framework), a joint resolution of Canada's Privacy Commissioners and Privacy Oversight Officials issued on February 5, 2008⁵ and existing privacy 'best practices'.

We understood that we would receive the PIA from SGI in approximately September 2008. As of March 5, 2009, we have not received the PIA.

/4

² S.S. 1990-91, c. F-22.01 as am.

³ S.S. 1999, c. H-0.021 as am.

⁴ Available at www.justice.gov.sk.ca/AP-Privacy

⁵ Available at www.oipc.sk.ca under the *What's New* tab.

As of this date we have not been consulted with respect to Bill 72. Neither was Bill 72 brought to our attention by SGI in our discussions about the PIA. This was notwithstanding our 2008 discussions with SGI and the July 30, 2008 news release from our office identifying that “*Enhanced Driver’s Licence raises some interesting privacy issues*”. A copy of that release is attached as is a related Leader Post story published on August 1, 2008.

Now that Bill 72 has received Second Reading and has moved to the Crown and Central Agencies for consideration, I am providing preliminary comments based on our understanding of the implications of the EDL to be offered by SGI to Saskatchewan residents. This commentary may need to be revised at such time as we receive and can review the PIA on this EDL initiative. I want to ensure that the Legislative Assembly is afforded an opportunity to consider significant privacy issues raised by some of the features contemplated for the EDL **before** it completes its consideration of Bill 72.

SASKATCHEWAN TAKES A DIFFERENT APPROACH

Bill 72 takes a very different approach than the corresponding enabling legislation seen in Manitoba. The Manitoba legislation is the latest of its kind by any Canadian jurisdiction and significantly improves the treatment of privacy concerns over earlier initiatives in British Columbia and Ontario. A different approach has also been taken in this province in regard to privacy issues engaged by reason of elements of the EDL program and the RFID chip technology. We understand that in B.C., Ontario and Manitoba, comprehensive PIAs were completed by government and shared with privacy oversight agencies well in advance of the enabling legislation or in the case of British Columbia prior to the launch of the EDL. In each of those three provinces, the privacy issues engaged by the EDL are acknowledged and explicitly addressed either in the statute in the case of Manitoba or in supporting literature in the case of British Columbia and Ontario. By contrast, Bill 72 appears to be silent on the privacy invasive technology that is part of the DHS specifications. Specifically, Bill 72 makes no reference to:

- radio frequency identification (RFID) tags,
- the privacy invasive character of RFID tags in this context,
- the risks to privacy associated with RFID tags,
- safeguarding the new database⁶ created by the EDL,
- an offence provision for failure to protect the personal information of Saskatchewan EDL holders,
- penalties for failure to protect that personal information of EDL holders,
- any provision to mitigate the significant privacy risks,
- any provision for the audit of collection, use and disclosure practices of SGI associated with RFID tags or the personal information collected at the time of application for the EDL.

⁶ For the first time SGI will be collecting, and using citizenship information on all applicants for the EDL.

I have not received any supporting documents or explanatory material from the Government that address these matters missing from Bill 72. I would encourage Government to ensure there is an opportunity for public comment and consultations prior to proclaiming the Bill 72 regulations.

Unlike Manitoba where it appears that regulations were published in draft form before the legislation was passed, we have no idea what features will be addressed by regulation in this province. In any event, given past declarations of the Saskatchewan government about the importance of privacy it would be disappointing if privacy issues were not addressed in the enabling legislation and considered only in subordinate legislation i.e. regulations. Those past declarations include statements made in the 2003 Privacy Framework and its directive that “*This Privacy Framework is designed to place Saskatchewan at the strongest possible privacy protection policy*”.⁷ The vision for the Privacy Framework was: “*Within Executive Government, a culture of privacy protection is fostered and developed by ensuring that personal information is: a) collected, used and disclosed only as required to carry out the government’s legitimate business and public interest mandates; and b) properly protected through the use of appropriate security mechanisms.*”⁸

I enclose a copy of the resolution adopted by Canada’s Information and Privacy Commissioners in Victoria in January 2008 on the question of the enhanced driver’s licence. That resolution included the following:

“...
5. *The Commissioners call on provincial and territorial governments to:*

- a. ensure that individuals participate in an EDL program on the basis of informed consent, with full disclosure to individuals of all privacy-related matters before they consent;*
- b. ensure that robust privacy and security are built into all aspects of EDL projects, including by conducting thorough privacy impact assessments and threat risk assessments at the outset;*
- c. ensure that their EDL programs comply with applicable local privacy legislation; and*
- d. consult early and meaningfully with their privacy commissioner or other responsible privacy oversight official on all aspects of any contemplated EDL program.”*

⁷ P. 6, Available online at www.justice.gov.sk.ca/AP-Privacy

⁸ Ibid., P. 12. Although SGI is a Crown corporation and not part of “Executive Government”, all Crown corporations have been required to meet the requirements of the Privacy Framework as a matter of government policy.

MANITOBA's *The Drivers and Vehicles Amendment, Highway Traffic Amendment and Manitoba Public Insurance Corporation Amendment Act*

Manitoba is the latest Canadian jurisdiction to enact legislation that enables the EDL. *The Drivers and Vehicles Amendment, Highway Traffic Amendment and Manitoba Public Insurance Corporation Amendment* (the Manitoba Act) appears to have built on features found in the British Columbia EDL program and Ontario legislation.

The Manitoba Act contains a number of features that warrant consideration by the Assembly including⁹:

- No person required by the Act to have a driver's licence is required to choose an enhanced driver's licence. [This underscores the feature that the EDL is voluntary not compulsory] sec. 10.1(1)
- It provides for an agreement between the Manitoba government and the Government of Canada or the USA to expressly meet the requirements of the WHTI. Sec. 31.1
- Importantly, it then requires that interprovincial agreement to address reasonable safeguards to protect the confidentiality, security, accuracy and integrity of the personal information and the privacy of the persons whom the personal information is about. Sec. 31.1(b)
- It is an offence for any person to contravene a requirement of an agreement made under this Act to protect the confidentiality, security, accuracy and integrity of records, personal information or personal health information about other persons, or the privacy of other persons. Sec. 122.1(c)
- Incorporation of the principles of data minimization i.e. limit the amount of personal information "to the minimum amount necessary to have the drivers' licences made." Sec. 128(2)
- Mandatory requirement that the agreement with the manufacturer of the EDL provide for the security of information by requiring reasonable administrative, technical and physical safeguards. Sec. 128(3).
- There is a similar requirement for any agreement with a person authorized to provide a service pursuant to section 1381(a) or (a.1) for security of information. Section 138(3)

⁹ Section number references are to the three statutes amended by the Act.

The foregoing items should not be considered an exhaustive list of improvements to Bill 72 and additional items may be identified after the PIA is received and reviewed.

In addition to the foregoing features there is a strong set of general provisions for records and information security in the Manitoba Act that has no counterpart in Bill 72. This includes a positive duty to adopt security safeguards.

The failure of Bill 72 to include many of these features is particularly troubling since our *The Freedom of Information and Protection of Privacy Act* is deficient by not including any requirement for Saskatchewan government institutions to take reasonable steps to safeguard personal information. This leaves the personal information of Saskatchewan residents that may be collected, used or disclosed as part of the EDL program at an unacceptable level of risk.

SOME INITIAL OBSERVATIONS ABOUT BILL 72

I make no comment on the portion of Bill 72 that deals with vehicles of volunteer firefighters and first responders.

The Bill's main focus would seem to be the mechanics of issuing, or refusing to issue, an enhanced driver's licence or enhanced photo identification card. It does not address in any transparent fashion the issues of privacy. Section 11 would amend subsection 287(1) of *The Highway Traffic Act* by prescribing the process the administrator must follow for the purpose of determining a person's eligibility for an enhanced driver's licence or enhanced photo identification card. This does not provide any direction in terms of addressing the obvious privacy issues engaged by the EDL. Specifically there is no stipulation that the EDL will be based on informed consent. That is emphasized in the Ontario and Manitoba statutes and in the information material in British Columbia. Section 11 also would revise subsection 287(1) of *The Highway Traffic Act* by prescribing the form and the content of an enhanced driver's licence or a photo identification card. Again there is no direction in terms of addressing privacy concerns.

This failure to explicitly deal with privacy considerations is disappointing given the considerable work done in other provinces to address privacy concerns. It appears that Saskatchewan is choosing to take a divergent approach out of step with those other Canadian jurisdictions. This failure is aggravated by the deficiency in FOIP outlined in my past Annual Reports¹⁰ - namely the omission is the failure in our FOIP Act to require government institutions such as SGI to take reasonable measures to protect personal information in their possession or control.

ASSESSING COMPLIANCE WITH FAIR INFORMATION PRACTICES

We assume that SGI will yet complete the proposed PIA on their EDL initiative. In the meantime, we offer some comments for the Assembly that may be helpful in its consideration of Bill 72. Our PIA form helps a government institution to consider privacy best practices as well as the legislative requirements. Privacy best practices also described as Fair Information Practices are represented by the *Model Code for the Protection of Personal Information*.¹¹ This was the basis for the Privacy Framework adopted by the Saskatchewan government in 2003. The headings below correspond to 6 of the 10 principles that comprise the Fair Information Practices.

1) ACCOUNTABILITY FOR PERSONAL INFORMATION

This requirement is that there be clear vesting of responsibility and a designated individual who is accountable for compliance with privacy requirements.

Without the SGI PIA, it is not possible to see how this key privacy principle is to be addressed in Saskatchewan's EDL. This may take a review of any agreements between the Canadian Border Security Agency and Saskatchewan which we haven't yet seen.

/9

¹⁰ 2003-2004 Annual Report, p. 21; 2004-2005 Annual Report, p. 14; 2005-2006 Annual Report, p. 17; 2006-2007 Annual Report, p. 2; 2007-2008 Annual Report, p. 4. There is a general obligation to "protect and maintain public records" included in the section 21(5) of the *Archives Act, 2004*. That however does not explicitly set out a specific duty to take reasonable measures to ensure there are technical, physical and administrative safeguards and further is not reinforced by provision for independent oversight, or by offence and penalty provisions that are common in public sector privacy legislation in other Canadian jurisdictions such as Ontario, B.C., Alberta, Newfoundland & Labrador, PEI.

¹¹ The Model Code for the Protection of Personal Information was developed by the Canadian Standards Association and is Schedule 1 to the federal *Personal Information Protection and Electronic Documents Act*(PIPEDA). There is a hyperlink to PIPEDA and Schedule 1 at our website, www.oipc.sk.ca.

2) COLLECTION OF PERSONAL INFORMATION AND IDENTIFYING PURPOSE

Collection shall be limited to that which is necessary for the purposes identified by the organization and information shall be collected by fair and lawful means.

This will require a review of documents not yet provided to us by SGI. The Manitoba Applicant's Guide may be a useful resource. Will additional information be collected in future EDL applications? If so, what uses will be made of that information? Is there any possibility that personal information beyond the assigned number will be added to the RFID chip?

3) CONSENT

With limited exceptions, the knowledge and voluntary consent of the data subject are required.

There is no assurance by virtue of Bill 72 that Saskatchewan residents who apply for an enhanced driver's licence will be provided with sufficient information about the RFID risks so that any consent they provide will be meaningful and informed. This includes recognition that the EDL is not required for any Canadian that holds a current passport.

Given the improvements undertaken by the federal Passport office, the process for obtaining a passport has apparently been much improved. I expect that the percentage of Saskatchewan residents who now have a passport is higher than would have been the case even a few years ago.

The passport does not utilize RFID technology. The EDL, as I understand it, is only useful for Saskatchewan residents who do not have a passport and who are not commercial vehicle operators who will most likely have utilized the NEXUS system to enter the U.S. and CANPASS to return to Canada. Although this will likely be addressed in the forthcoming PIA, it does not appear from the U.S. Customs and Border Patrol website that there are significant traffic volumes and delays at the eight border crossing points in Saskatchewan. The EDL is not useful for air travel to the United States for which a Canadian passport will still be required.

To the extent that the EDL program in Saskatchewan is voluntary, participants must be provided with full and clear information at the time of applying. Any Participant Guide must make it clear that EDL holders' personal information may be disclosed according to USA law and that it is not protected by Canadian federal or provincial privacy legislation once it has been disclosed by the Canadian Border Security Agency to the U.S.A. Customs and Border Security.

There must be sufficiently detailed information to ensure that any consent obtained from applicants is fully informed and meaningful. It should identify risks associated with the USA Patriot Act and the fact that Canadian and Saskatchewan privacy laws and the reach of Canadian and Saskatchewan Privacy Commissioners does not extend to the U.S.A. There is also nothing comparable in the U.S.A. to either the general privacy legislation or independent privacy oversight officers accountable to Parliament or the Legislative Assembly.

4) LIMITING USE, DISCLOSURE & RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with consent or as required by law. Personal information shall be retained only as long as necessary.

This information is highly sensitive. Bill 72 deals with identity documents or 'foundation documents' that are of enormous value to identity thieves and all kinds of commercial organizations. There are questions about how this personal information of Saskatchewan residents will be stored, safeguarded, used and disclosed to federal agencies.

I am concerned about the proliferation of databases containing images of the foundation documents and application information on EDL participants. Will personal information about EDL participants be potentially held in separate databases by SGI, its information management service providers, Canadian Border Security Agency, Canada Immigration, USA Customs and Border Security and the USA Department of Homeland Security? In addition, if the individual holding an EDL also holds a Canadian passport, identical information would also be available in the Passport Canada database. Duplication of these files, containing valuable foundation documents is likely to increase the risk of inappropriate disclosure, theft and misuse.

Our office generally recommends against duplication of files and databases containing personal information unless this is essential.

5) ACCURACY

Personal information shall be accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

This requires a careful review of the PIA when it is furnished to determine whether there will be appropriate opportunities and procedures for applicants to verify and correct the information in their files.

Will there be an opportunity for individuals to request corrections to their information after it is transferred to USA Customs and Border Protection?

6) SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

The anticipated PIA will presumably include the SGI business plan which hopefully will document a threat and risk assessment of the internal environment, staff training, audit trails and security processes.

We have concerns with the use of vicinity as opposed to proximity RFID technology in the EDL chip. The “vicinity read” or long-range GEN-2 RFID technology renders both the data and the location of the individual vulnerable. Our clear preference would be for close proximity RFIDs with much shorter antennae. I note that the International Civil Aviation Organization standards for chips used in electronic border crossing documents is to utilize proximity technology and be readable at a distance of 10 centimetres.

The model of the EDL implemented in British Columbia is a vicinity reader and not a proximity reader. This allows the RFID tag to be read up to 50 metres away. That raises the question of what would stop a criminal from walking through Mosaic Stadium during a Rider home game while remotely reading EDLs that anyone may be carrying in their wallet or purse and collecting those numbers assigned by the Canadian Border Security Agency. Even if the only personal information that can be read remotely in that way is the number assigned to the holder of a particular card, that number is the personal information of the holder by reason of section 24(1)(d)¹² of FOIP. The British Columbia model does not have an on/off switch although we understand that this may be a feasible feature that could be included.

/12

¹² Personal information means personal information about an identifiable individual that is recorded in any form and includes: ... (d) any identifying number, symbol or other particular assigned to the individual, other than the individual’s health services number as defined in *The Health Information Protection Act*.

In British Columbia, the EDL is accompanied by a Faraday sleeve¹³ to minimize the risk. The sleeve is an imperfect solution since it may be destroyed or forgotten by the licensed driver. It is only a secure solution when the cardholder remembers to place the card in the sleeve. Otherwise the reading of the cards becomes free and clear. This feature also puts all of the burden of privacy protection on the Saskatchewan resident. It is likely that the EDL will be used in many ways where driver's licences are now required to establish identity or proof of age. This may be at a retail outlet, an office of some service provider or to set up a utility account. In all of these cases, the cardholder is removing the card from the Faraday sleeve. That has the effect of exposing the information on the card.

I understand that EDLs will still need to be physically presented to the Customs Border Protection agent on a one-to-one basis at a border crossing. If it still means that a Saskatchewan resident must drive her vehicle to the border crossing, wait for a border agent to speak with her and hold the card up so it can be read by the border agent, it would seem that a proximity read tag is all that would be required.

The risks with vicinity RFIDs include skimming for fraud purposes. In addition there is the risk of tracking and surveillance of RFIDs without the knowledge of the traveler. Long range or vicinity RFID technology was not created for purposes of human identification and tracking, but for object location and identification. For that reason, vicinity RFID technology was not designed with individual rights, data protection, or privacy in mind.

A NEW NATIONAL IDENTITY CARD

Since the announcement of the enhanced driver's licence initiative by British Columbia and the Canadian Border Security Agency, commentators have speculated that the EDL may be the foundation for a new electronic identity card that all Canadians will be required to carry. This is a very large issue and one that warrants much more discussion than this submission affords. Suffice it to say that a single national identity card carries huge risks for the security of any Canadian's personal information. I encourage the Assembly to be clear with Saskatchewan residents that this EDL project is not a foundation for a new national identity card.

¹³ Also referred to as the Faraday cage

RECOMMENDATIONS

- 1. That Bill 72 be revised to explicitly recognize the privacy concerns associated with the EDL and that the Assembly should consider a number of privacy-positive features discussed in this submission.**
- 2. That Bill 72 be revised to specifically require that SGI take all reasonable measures to ensure the personal information collected, used or disclosed is adequately protected by means of physical, technical and administrative measures.**
- 3. That such a duty to safeguard information be reinforced by an offence provision and a serious penalty in the order of penalties in *The Health Information Protection Act*.**
- 4. That a detailed and thorough Privacy Impact Assessment be provided to our office without delay in order that we can provide our advice to the Assembly.**
- 5. That the Assembly ensures that the radio frequency identification device utilized in Saskatchewan should be a proximity device instead of a vicinity device.**
- 6. That the Assembly consider the importance of ensuring that any consent associated with an application for an EDL or identity card be a fully informed consent.**
- 7. That the Assembly consider requiring that the EDL or identity card contain stronger security than that offered by the Faraday sleeve. Ideally, this would involve an on/off switch to be operated by the EDL or identity card holder.**
- 8. That Saskatchewan carefully considers the information and materials that have been developed in other jurisdictions, particularly Manitoba, and determine how those materials could be adapted for Saskatchewan.**
- 9. That any regulations, information tools, brochures be provided to our office in draft form in a timely way to enable us to provide input before roll-out of the EDL/identity card program.**
- 10. That any regulations be published in draft form to permit public comment before they are proclaimed.**

Honourable D. Toth
March 5, 2008
Page 14

I trust that this commentary will be useful to the Assembly in its consideration of Bill 72.

All of which is respectfully submitted,

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner
Enclosures: (4)