Information and Privacy
Commissioner of Ontario

Commissaire à l'information
et à la protection de la vie privée de l'Ontario

Submission from the Information & Privacy Commissioner/Ontario on Bill 85, *An Act to permit the issuance of photo cards to residents of Ontario and to make complementary amendments to the Highway Traffic Act*

October 2008

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Introduction

Thank you for providing the Office of the Information and Privacy Commissioner of Ontario with the opportunity to comment on Bill 85, *An Act to permit the issuance of photo cards to residents of Ontario and to make complementary amendments to the Highway Traffic Act*. This *Act* is also commonly referred to as the *Photo Card Act, 2008*.

I am providing you with comments under section 59(a) of the *Freedom of Information and Protection of Privacy Act (FIPPA)*, which states that the Information and Privacy Commissioner may offer comment on the privacy protection implications of proposed legislative schemes or government programs.

As Ontario's Information and Privacy Commissioner, my mandate encompasses many responsibilities, such as, overseeing compliance with Ontario's privacy and access legislation. Providing counsel on the privacy implications of proposed legislation or sweeping technological changes to government is also important to my Office. The public should understand this new photo card program and the implications of the proposed legislation when they apply for one of these photo cards.

The primary purpose behind the proposed *Photo Card Act, 2008* is to enable the government to issue an enhanced driver's licence (EDL) that will serve as an alternative to a passport solely for entering the United States. In addition, the proposed legislation provides the government with the authority to issue new photo cards for those who do not, or cannot, hold a driver's licence – such as people who have a severe visual impairment. These photo cards are already available in most provinces. To parallel the EDL, Bill 85 also allows the government to enhance these photo cards to serve as an alternative to a passport when travelling to the United States.

I further understand that these efforts to introduce an alternative border crossing document for Canadian citizens in Ontario is to meet the U.S. government Western Hemisphere Travel Initiative (WHTI) that has grown out of security concerns regarding the events of 9/11. WHTI is a result of a requirement in the U.S. *Intelligence Reform and Terrorism Prevention Act of 2004*, and directs the Department of Homeland Security (DHS) to devise a plan for additional safeguards relating to border identification (ID) requirements. WHTI affects categories of individuals for whom documentation requirements have previously been waived, such as Canadians. As a result, by June 1, 2009, Canadians will either have to present a passport at U.S. land and sea ports of entry, or a passport alternative that is acceptable to DHS.

As an individual citizen, I understand concerns about the growth of terrorism. However, as Ontario's Information and Privacy Commissioner, I also fear the potential loss of our freedoms, especially privacy, which I believe, forms the basis of all of our other freedoms.

In the period following 9/11, many citizens, especially those in the U.S., were hesitant to speak out on behalf of privacy because it would somehow be viewed as being unpatriotic. Shortly after, I issued a position paper entitled, *Public safety is paramount - but balanced against privacy*, in response to a request from the CBC. The position was that we have to protect the safety of the public but we also have to ensure that any security measures undertaken were truly needed and effective. Let us not just give up our privacy, our freedom, for the mere *appearance* of security – it must be real. I fear that in the long-term, in our search for safety and security, we may end up forfeiting privacy. This would be a fundamental error, setting a precedent capable of unwinding centuries of progress in the evolution of a democratic society. Privacy is absolutely fundamental to freedom.

I want to state here that, for the record, I am not opposing the Ontario government's commitment to introduce an alternative border crossing document to the Canadian passport. I just want to make sure that privacy is built into it.

Over the past year, my Office has developed a positive working relationship with the Ministry of Transportation (the Ministry), Ontario's Intergovernmental Affairs and Cabinet Office, who have been keeping us informed of the implications of WHTI and its plans to implement an alternative border crossing card acceptable to the U.S. government.

We have also been quite proactive in advancing the forward momentum of this initiative. This past summer, I had the opportunity to co-host with Professor Andrew Clement, a public information forum on the privacy and security issues involving the EDL. We heard arguments from both sides of the debate, including from the University of Toronto's, Identity, Privacy and Security Initiative (IPSI), as well as representatives from both the provincial and federal governments. This multi-stakeholder input was very helpful in clarifying various elements of the EDL initiative.

On separate occasions, the Ministry also notified and continued to update my Office of its intent to introduce photo comparison technology as another mechanism to improve the quality of its driver's licence database by helping to: prevent fraud, support a "1 licence: 1 driver scheme" and, by extension, to ensure that there are no holders of both a photo card and a driver's licence. I understand the government's efforts to address the Provincial Auditor's recommendations to improve the accuracy of the driver's licence database by introducing, among other approaches, photo comparison technology.

The outline for this submission is as follows:

1. Overview of the types of photo cards and their purpose under Bill 85;

2. Review of the privacy and security issues of the proposed Enhanced Driver's Licence and Enhanced Photo Card (Citizenship verification and the use of RFID technology);

3. Comments on Bill 85 clauses (including clauses on the basic photo card and the Ministry's proposed use of photo comparison technology);

4. Conclusion;

5. Summary List of Recommendations.

1. Overview of the types of photo cards and their purpose under Bill 85

Bill 85 contemplates the issuance of three new photo cards by the Ministry and importantly states that there is no obligation for anyone in Ontario to obtain a photo card. Two of these cards may be used for travel by land or sea to the United States. The **driver's licence** will continue to be issued under the *Highway Traffic Act*.

A **"combined photo card,"** or what has been known as an **enhanced driver's licence (EDL),** will be both a driver's licence and a U.S. land or sea border crossing document. It will contain all the information currently found on a driver's licence as well as Canadian citizenship information and additional information about the holder that may be prescribed by the government. It will also be embedded with an RFID tag.

A **"basic photo card"** will be issued to individuals who, for whatever reason, do not or cannot have a driver's licence, to facilitate them carrying on routine activities requiring government-issued photo identification. It will contain the holder's name and photograph and additional information about the holder that may be prescribed by the government.

An **"enhanced photo card"** (EPC) is a basic photo card with added features similar to the combined photo card or EDL (Canadian citizenship information and RFID tag) that will also serve as a U.S. land or sea border crossing document.

2. Review of the privacy and security issues of the proposed Enhanced Driver's Licence (EDL) and Enhanced Photo Card (EPC)

Section 4(1) of Regulation 460 under *FIPPA* imposes a duty on each institution to "ensure that reasonable measures to prevent unauthorized access to the records in [the] institution are defined, documented and put in place, taking into account the nature of the records to be protected" and 4(2) provides, "Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it." These provisions put the onus on the institution to be accountable and to practice responsible information management.

2.1 Citizenship verification – database duplication

Earlier this year, I issued a press release to outline one of my main concerns regarding the security risks of the proposed EDL program. I respectfully asked that the Government of Canada securely provide citizenship information on naturalized citizens to Ontario to avoid the need to create a duplicate process of verifying citizenship for Canadians who apply for an EDL in Ontario. This proposal is not suggesting a new or impossible process. On the contrary, there are several precedents of secure information sharing between the federal and provincial governments to ensure authenticity and accuracy of the information. One such example is Ontario's Guaranteed Annual Income Supplement (GAINS) program which receives tax status information from the federal Canada Revenue Agency on program applicants.

Some time ago, I also initiated a dialogue with The Honourable Stockwell Day, Minister of Public Safety and responsible for national coordination of the EDL initiative, to find a way for Citizenship and Immigration Canada (CIC) to securely verify citizenship for Ontario's EDL initiative.

Further, in early correspondence with the Ontario Deputy Ministers of Transportation and Intergovernmental Affairs, I made note of the fact that when it comes to responsible information management, the practice of data minimization should always prevail. Requiring provinces to build their own new databases of citizenship information – in effect reinventing the wheel – needlessly adds to privacy and security concerns, not to mention, the unnecessary costs of a cumbersome and highly duplicative process. Simply put, the federal government does not need to waste valuable resources and taxpayer dollars by requiring Ontario to duplicate existing federal government processes.

Creating a mirror database of citizenship information already held by the federal government could very well serve to propagate identity theft and add to the potential of unintended consequences, of error and inaccuracy, that would arise in the process of recreating existing citizenship information. Ontario's database would not consist of a simple "yes-no" for citizenship. Rather, the database would need to contain the answers and notes to a lengthy in-person interview with each applicant. And the process may not end there for an applicant. If the interview questions reveal a complicated situation, the matter is to be forwarded to federal government staff, in any event, resulting in further duplication, cost and privacy risk. This duplicate process is no simple matter, and can result in an unnecessary and detailed database of highly sensitive personal information.

I know this is a federal issue and not the Premier or Minister's doing. But in my view, it is an important matter that must be resolved. The federal government already has this information. It clearly has the ability to easily verify the citizenship of naturalized Canadians, and securely provide that information to a province, such as Ontario, upon

request. This would clearly be a more privacy-protective and cost effective model – a "win/win" scenario.

Recommendation 1: The Ontario government must strongly pursue the federal government to take responsibility for verifying the citizenship status of naturalized Canadian citizens and providing that information to Ontario for the purpose of the Enhanced Driver's Licence and Enhanced Photo Card. Ontario cannot create a new collection and retention of personal information already existing in the hands of the federal government. The principle of data minimization must be observed.

2.2 Radio frequency identification (RFID) technology

2.2.1 RFID and U.S. border crossing photo cards

RFID technology is a generic term for a variety of wireless technologies that use radio waves for purposes of identification and consists of two integral parts: a tag and a reader.

There are also two main types of RFID tags: active or passive. The difference depends on whether the tag has its own power system or not. Passive tags have no power source and no on-tag transmitter.

Finally, all RFID tags are activated by readers, which in turn are connected to a host computer. In a passive system, the RFID reader transmits an energy field that "wakes up" the tag and powers it, enabling it to transmit data.

I have spent many years working in this field, trying to secure privacy within RFID technology, and I have produced four papers and a set of practical tips on this subject. I am not opposed to the use of RFID tags – indeed, they can have many benefits. But, like all information communication technologies (ICTs), they need to have privacy issues baked in early within the design of these systems – or what I commonly refer to as "privacy by design."

While tagging things in such areas as the supply chain management system or taking inventory of assets raises no privacy concerns, *tagging things linked to people* can present issues because of the relative permanence of the tag, the nature and amount of the data collected, and the strength of the data's linkage to identifiable individuals, in addition to the sensitivity of the linked data. Once you have the possibility for data linkage to identify individuals, that is when privacy concerns arise.

The U.S. government has mandated that any new border-crossing document, such as Ontario's proposed enhanced driver's licence and the enhanced photo card, include RFID technology. The reason becomes more evident when tracing the history of RFID use by the U.S. government. According to an official U.S. government document, U.S. Customs

and Border Protection (CBP) uses RFID technology on its trusted or registered traveler programs (e.g. NEXUS, SENTRi, FAST, Passport Card) at designated land border sites, in order to "expedite the processing of pre-approved, international, and low-risk commercial and commuter travelers crossing the border."[1]

The RFID tag will store a unique index number to a database file, rather than a copy of the information printed on the card. By using an Ultra High Frequency (UHF) vicinity-read RFID tag that has a typical read range of 15 feet (roughly five metres), the U.S. government anticipates that, in advance of a traveler's arrival at the inspection booth, border-crossing officers will be able to quickly access traveler information from a government database (including screening through various watch lists) without impeding traffic flow. The U.S. also expects that the RFID technology will allow multiple cards to be read at a distance and simultaneously as would be the case when there are several passengers in a car or van.[2]

Arlene White, Executive Director for the Binational Tourism Alliance, a not-for-profit trade organization created to support tourism in cross-border regions shared by Canada and the United States, spoke at the summer EDL Forum about these border communities and their support for this program to ensure the smooth flow of traffic at the borders.

2.2.2 RFID privacy and security issues

There are well-known privacy and security vulnerabilities associated with RFID technology. [3,4]

Very briefly, these are:

- **eavesdropping** - which occurs when an unauthorized individual intercepts data while an authorized RFID reader is reading the data;
- **skimming** - which occurs when an individual with an unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge;
- **cloning** - which occurs when the original RFID chip and its data are duplicated.

These vulnerabilities could lead to a host of undesirable consequences such as identity theft, unauthorized identification, and covert tracking and surveillance of individuals.

In response to these privacy concerns, one may hear that the RFID tag does not include any personally identifiable information, only a unique number linking the cardholder to

[1] Department of Homeland Security, Office of Inspector General. *CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security (Redacted)*. Report OIG-06-36 , May 2006, p. 4.
[2] *U.S. Passport Card FAQ's*. http://travel.state.gov/passport/ppt_card/ppt_card_3921.html?css=print
[3] Harris/decima. *Research on Alternative Documentation for Land and Sea Travel*, September 20, 2007.
[4] *Radio Frequency Identification Technology in the Federal Government,* GAO-05-551, May 2005.

his or her record in a database, so no privacy concerns arise. However, this is incorrect. A number, when uniquely linked to an individual, is not inconsequential – it is not just a meaningless number – it points to real, personally identifiable information. A Social Insurance Number, a passport number or a driver's licence number – while each of these unique identification numbers may appear to be "just a string of numbers," "of no use to anyone," when linked to personally identifiable information, each can be misused, by unauthorized persons or used for unintended purposes that may cause real harm to real people. Identity theft is a case in point. It is on the rise and is now considered by both Canadian and American law enforcement agencies to be the fastest growing form of consumer fraud in North America – a great deal of which is due to organized crime.

Regardless of the contents of the data stored on the RFID tag, if that data is both a unique identifier and accessible via an unauthorized reader (or network of readers), then the cardholder's identity may be ascertained, and the individual can then be tracked without his or her knowledge. Even if the data on the card cannot be associated with *existing* personal information about the cardholder (i.e., the database of personal information remains secure), it may be used to collect personally identifiable information over time.

One significant consideration that must be recalled in the development of any RFID-based project, and particularly one with a great deal of sensitivity such as the EDL or EPC, is the testing phase of the project. In the U.S., the DHS Office of Inspector General has audit and oversight responsibilities, and undertook an audit of the DHS' systems for utilizing RFID technology. We have moved away from the possibility of a single person, or department, being able to sit down and understand the entirety of this technology's impacts – there is a need now for independent third-party testing and evaluation of the system, *prior* to deployment.

Recommendation 2: To assure the Canadian public of the government's commitment to protecting their personal information and identity when implementing an RFID technology system, there must be an independent privacy audit and end-to-end threat risk assessment that adequately identifies and addresses any privacy and security issues.

Recommendation 3: Any use of RFID technology by the Ontario government must comply with the RFID guidelines developed by the Office of the Information and Privacy Commissioner of Ontario.[5]

2.2.3 RFID privacy protection - faraday cage vs. on/off switch

The federal government will be required to address the security and privacy issues related to the RFID technology system when the EDL or EPC is used at the border (e.g. protection of the federal database of EDL/EPC applicant information, security of the

[5] *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, by Ann Cavoukian, Ph.D., Commissioner, June 2006, available online at http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf

transmission between the U.S. border readers and the federal database, etc.). However, in their daily activities away from the border, Ontarians who hold one of these cards may have remaining apprehensions about the privacy and security issues associated with the fact that an RFID tag can be read by an unauthorized reader or readers and be used to track or covertly survey their activities. It is important that the Ontario government provide these cardholders a means of controlling the transmission of the data by the RFID chip on the EDL or EPC and offer a measure of privacy from unauthorized identification, tracking and surveillance when the card is not in use.

Currently, the suggested method for allowing cardholders a measure of privacy and security is to provide them with an "electronically opaque" protective sleeve, called a Faraday Cage, which would prevent communications to and from the RFID chip, when the card is encased in the sleeve.

The proposed protective sleeve, when offered as the only privacy measure, would mean that the card would allow, by default, the collection of stored data by unauthorized RFID readers, until the cardholder remembered to place the card in the protective sleeve. This is only a secure solution when the individual remembers to place the card in the sleeve – otherwise the reading of the cards becomes free and clear.

Leading researchers such as Sophia Cope, staff attorney and a fellow at the Center for Democracy and Technology, a non-profit public policy organization in Washington D.C., agree that this method is hardly sufficient. In her testimony before a Senate Committee on the implementation of the *REAL ID Act* and the Western Hemisphere Travel Initiative (WHTI), Ms. Cope stated that privacy risk mitigation measures such as the Faraday Cage,

> *"…improperly place the burden of privacy protection on the citizen. Moreover, they offer no protection in light of the fact that the EDL and the passport card will be used in many circumstances where driver's licenses or ID cards are now required, including in many commercial contexts, where individuals will be taking their cards out of the protective sleeve, thereby exposing their data to all the risks we have described above."*

In Ontario, people often use their driver's licence when asked for a government issued photo ID – to vote, to open a bank account or apply for a credit card, or as proof of age in convenience stores or bars.

As the RFID standard chosen for this project will respond to any reader query, the card must have some means of preventing it from being read when not required – a better solution than the proposed protective sleeve is needed.

The best choice would be to give the cardholder the option of physically verifying the selected transmission setting. That is, adding the equivalent of an "on/off" switch to the RFID, which can be incorporated directly into the card.

This proposal is not based on "yet-to-be-developed" technology. The MIT Media Lab has already patented and prototyped an "on/off switch" for the RFID tag that can be incorporated directly into the card, which allows the card holder to determine when and where his or her information can be transmitted.

So has another company based in the U.K. – Peratech, a company that has developed an on/off switch using Quantum Tunneling Composites technology (QTC). Its founder and CTO David Lussey advises that, "*Peratech's technology is readily available under license for the application of acting as an on/off switch on an RFID driver's license. It has been fully proven to work reliably in the typical hot-lamination manufacturing process as used by all the major RFID card manufacturers. And it is just a matter of cents, not dollars that we are talking about*."

There is also another U.S. company – Root Labs -- which is working on a similar switch that can be placed on the transponder used by San Francisco Bay area highway toll users.

We believe an on/off switch technology for the EDL and EPC should be available for Ontarians. Our office brought together Ontario government staff and the vendor selected to produce the EDL and EPC in Ontario, hoping to advance the case for including this very promising technology on behalf of those who may want to apply for an Ontario Enhanced Driver's Licence or Enhanced Photo Card.

In fact, a senior executive, from the government's selected vendor for the cards, has stated that, "*We are aware of the developments of new and emerging technologies that provide the means to personally control RFID transmission of data with an on/off switch on a card, such as Peratech's QTC technology. Furthermore, Giesecke & Devrient (G&D) is working diligently on the development of our own technologies and assessment of such third-party technologies to enhance RFID functionality, security and also privacy.*"

Recommendation 4: The Ministry must work with a selected vendor to pursue adding a privacy-enhancing on/off switch for the RFID tag embedded in the card.

3. Comments on Bill 85 clauses

This section focuses on recommendations on the language of Bill 85 in order to help the Ministry better align the proposed legislation, as written, to the intent of the Ministry's announced EDL and EPC. I am confident that by working together, the Ministry and my Office will be able to address these recommendations.

Our recommendations focus on four of the broadly recognized fair information principles that are embodied in *FIPPA* as follows:

1) the accountability principle;
2) the purpose identification and limitation principle;

3) the collection limitation and data minimization principle;
4) the use and disclosure limitation principle.

As a fair information principle, *accountability* requires an institution that is responsible for personal information to remain responsible for the information throughout its life-cycle (collection, use, disclosure, retention, disposal), even if such information is shared with or transferred to a third party agent of the institution. Institutions are required to use contractual or other means to provide a comparable level of protection while the information is in the hands of a third party.

The *purpose identification and limitation* principle requires the institution collecting personal information to identify the purposes for which the information is collected and to use or disclose the information only for those purposes. This principle is intended to prevent "function creep" (systems designed for one purpose extended over time to other purposes not originally intended) because identifying the purpose of collection enables institutions to determine what information they need to fulfil those purposes.

The *collection limitation and data minimization* principle requires that the personal information collected be limited to only that which is necessary to fulfil the purposes of the collection.

The *use and disclosure limitation principle* requires that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

3.1 Accountability

3.1.1 Agreements with third parties

Accountability requires that when personal information is disclosed to others, the public should have the assurance that appropriate agreements will be put in place to protect their privacy and security.

Under Bill 85, the Ministry will have direct responsibility for ensuring the privacy and security of the personal information collected, used and disclosed for the photo card programs. As such, the Ministry should be required by Bill 85 to seek equivalent privacy protection through contractual or other means when disclosing or transferring personal information to third parties. This principle is reflected in section 21, 42 and 65.1 of *FIPPA*, section 14 and 3 of *MFIPPA*, as well as in other statutes mentioned below - but not in Bill 85.

Assurances have been given that a Memorandum of Understanding (MOU) will be signed between the Ontario Government and Canada Border Services Agency (CBSA), and that

an MOU has been signed between the Canadian Government and U.S. authorities. Ontario cannot enforce its laws in other jurisdictions. As a result, the only assurance that Ontario residents can have that adequate protections will be given to their privacy is through agreements between Ontario institutions that disclose information and the entities that receive it. Bill 85 contains no requirement to enter into such agreements.

This type of protection exists in several other Acts including in Ontario, the *Personal Health Information Protection Act, 2004* (*PHIPA*).

Section 39 of the *Personal Health Information Protection Act, 2004* provides that personal health information may only be disclosed to an auditor if the auditor signs an agreement that the records will be held in a secure and confidential manner and will be returned when the audit is completed. Section 42 of *PHIPA* provides that a health information custodian may disclose personal health information to a potential successor only if the potential successor signs an agreement to keep the information confidential and secure, and not to retain any of the information longer than is necessary under other Ontario statutes for the purpose of the assessment or evaluation of the business.

Similar provisions are found in *FIPPA* and *MFIPPA*, as well as Ontario's *Highway 407 Act, 1998*; *Highway 407 East Completion Act, 2001*; *Financial Administration Act*; *Long-Term Care Homes Act, 2007*; *Trillium Gift of Life Network Act*; *Compulsory Automobile Insurance Act*; and several other Ontario statutes.

Statutes such as the *Health Insurance Act,* and *the Ontario Works Act, 1997* for example, require that disclosure agreements contain other safeguards as well as those described above.

Recommendation 5: Bill 85 should be amended with language similar to Sections 39 and 42 of *PHIPA* to require that any authorized disclosure of personal information to other Ontario institutions not covered by *FIPPA* and *MFIPPA*, other territorial or provincial governments, the Government of Canada, or any agency of the Government of the United States, only be made subject to an appropriate agreement that safeguards the personal information.

Recommendation 6: Bill 85 should set out the minimum contents of such disclosure agreements. For example, the agreements must provide for transferring the minimum amount of information (otherwise known as data minimization), and for monitoring and auditing of compliance. Except to the extent of legitimate security needs for the confidentiality of certain clauses, the full agreements should be made readily available to the public.

3.1.2 Deemed compliance provisions

As stated above, it is crucial that legislation authorizing transfers of personal information to other jurisdictions require that these transfers only be made subject to agreements to ensure confidentiality and security of the information. Not only does Bill 85 fail to provide for such agreements, but it actually contains two provisions that do away with any requirement to enter into such agreements. Sections 11(5) and 44 (complementary amendment to the *Highway Traffic Act*) at 205.0.1(5) of Bill 85 state:

> (5) Any disclosure of information under this section is deemed to be in compliance with clause 42 (1) (e) of the *Freedom of Information and Protection of Privacy Act* and clause 32 (e) of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*.

These provisions override sections 42(1)(e) of *FIPPA* and 32(e) of *MFIPPA*, which state that an institution shall not disclose personal information except for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder. Bill 85 exempts disclosures by and to the Ministry from this requirement. In doing so, the Ministry will be able to disclose information without the safeguard of an agreement. If the Ministry intends to disclose information only under an agreement, then the deeming provision is not necessary. In addition, it is not sufficient as a justification that the Ministry would include a deeming provision simply because it is unable to anticipate all future scenarios in which disclosures of information may take place.

These provisions of Bill 85 impede the rights of individuals to control the disclosure of their personal information and represent a serious infringement on the privacy rights of these individuals. Such provisions frustrate the objectives of *FIPPA* and *MFIPPA*, namely, to allow individuals to exercise control over the disclosure of their personal information by government institutions.

These deeming provisions also defeat the independent oversight of the collection, use and disclosure of personal information by government, which is entrusted to my Office. Moreover, these provisions are inconsistent with section 43 of *FIPPA* and section 33 of *MFIPPA,* which state that personal information can only be used or disclosed for a consistent purpose if the individual might reasonably have expected such a use or disclosure. Canadian citizens in Ontario, who provide their personal information to the Ministry for the purposes of expediting border crossing cannot reasonably expect all the unspecified uses and disclosures that may occur pursuant to Bill 85.

Recommendation 7: Bill 85 should be amended to delete subsections 11(5) and 205.0.1(5) (contained at s. 44 of Bill 85) so that sections 42 of *FIPPA* and 32 of *MFIPPA* will apply to disclosures of information.

3.1.3 Immunity from liability

Collection of personal information and accountability for this information under an institution's control entails a duty of care for its protection. Section 21(1) of the bill includes government immunity from liability for damages regarding anything done in good faith in the performance of a duty under the *Act,* or any neglect or default in the performance of a duty or power. Similarly, subsection 21(2) immunizes the government from liability for damages public servants or persons authorized by the Ministry for use of the photo card or information on such card. Unlike subsection (1), subsection (2) does not include a requirement of good faith for the immunity to be effective. Also, contrast 21(2) with the protection from personal liability contained in the amendments to the *Highway Traffic Act* at s. 29 of Bill 85, which also contains a requirement of good faith.

This immunity is drafted too broadly and does not provide appropriate protection for Ontarians who become the victims of government negligence in the handling of their personal information under the various photo card programs.

Recommendation 8: Subsection 21(2) of Bill 85 should be amended to include a standard of good faith.

Recommendation 9: Bill 85 should be amended to add a subsection (3) to s. 21 that mirrors the wording of 5.4(2) at s. 29 (amendment to the *Highway Traffic Act*).

3.1.4 Openness and transparency - public consultation on regulations

Openness and transparency are key to government accountability, especially when the government serves as custodian of a significant amount of personal information on its citizens. Bill 85 leaves crucial matters affecting the privacy and security of Ontarians either to the discretion of government officials or to be later prescribed by regulation, without any requirement for public notice or comment.

These matters include:

1) the information to be contained on the photo card;
2) the security and other features that may allow the photo card to be used for travel;
3) the information that the Ontario government will collect from municipalities and other provincial, territorial and federal government departments and agencies;
4) the information that the Ontario government will provide to municipalities and other provincial, territorial and federal government departments and agencies;
5) the contents of information-sharing agreements; and
6) the requirements for being issued a photo card.

Under these circumstances, we believe that in order for transparency and accountability to be achieved, the regulation-making powers in Bill 85 must allow for public consultation before a regulation is enacted. This would not be the first time in Ontario that such consultation is set out in legislation. These include *FIPPA*, *PHIPA*, the *Environmental Bill of Rights*, and the *Occupational Health and Safety Act*. The *Environmental Bill of Rights* provides for public consultation in regard to regulations made under 23 prescribed statutes administered by several ministries.

As government officials and public servants, we feel that we must provide an opportunity for the people of Ontario to voice their thoughts regarding a decision that may impact their lives and the government's collection, use and disclosure of their personal information. In my recommendation, we suggest specific wording to accomplish this based on the wording contained in *FIPPA* and *PHIPA*.

Our recommended wording differs from the wording in *FIPPA* and *PHIPA* in two respects. First, while we appreciate the need to forego public consultation in situations of urgency, we question whether the Minister should have the power to curtail public consultation because he or she is of the opinion that the regulation is "minor" or "technical." A regulation that appears to be minor to one person may be recognized by another to have major unintended consequences. The possibility of unanticipated impacts is one of the reasons that it so important to create an opportunity for public consultation. The fact that a regulation is "technical" is also not a sufficient reason to curtail public consultation. Many of the steps required to secure sensitive personal information, particularly in relation to biometrics, RFIDs, and electronic databases and data transfers, are technical in nature. This does not mean that the public cannot comment meaningfully on such regulations.

Secondly, we are not recommending the importation of the provisions in *FIPPA* and *PHIPA* that curtail the right to seek judicial review of the Minister's decisions under this Act. Under Ontario's *Judicial Review Procedure Act*, any decision taken pursuant to a statutory power of decision is normally subject to judicial review, and there is no time limit for initiating a judicial review application. It is not clear why these provisions should be an exception to this general rule.

Recommendation 10: Bill 85 should be amended to provide for public consultation before regulations are promulgated as follows:

(1) Subject to subsection (7), the Lieutenant Governor in Council shall not make any regulation under section 22 unless,

> *(a) the Minister has published a notice of the proposed regulation in The Ontario Gazette and given notice of the proposed regulation by all other means that the Minister considers appropriate for the purpose of providing notice to the persons who may be affected by the proposed regulation;*

(b) the notice complies with the requirements of this section;

(c) the time periods specified in the notice, during which members of the public may exercise a right described in clause (2)(b) or (c), have expired; and

(d) the Minister has considered whatever comments and submissions that members of the public have made on the proposed regulation in accordance with clause (2)(b) or (c) and has reported to the Lieutenant Governor in Council on what, if any, changes to the proposed regulation the Minister considers appropriate.

(2) The notice mentioned in clause (1)(a) shall contain,

(a) a description of the proposed regulation and the text of it;

(b) a statement of the time period during which members of the public may submit written comments on the proposed regulation to the Minister and the manner in which and the address to which the comments must be submitted;

(c) a description of whatever other rights, in addition to the right described in clause (b), that members of the public have to make submissions on the proposed regulation and the manner in which and the time period during which those rights must be exercised;

(d) a statement of where and when members of the public may review written information about the proposed regulation;

(e) all prescribed information; and

(f) all other information that the Minister considers appropriate.

(3) The time period mentioned in clauses (2)(b) and (c) shall be at least 60 days after the Minister gives the notice mentioned in clause (1)(a) unless the Minister shortens the time period in accordance with subsection (4).

(4) The Minister may shorten the time period if, in the Minister's opinion, the urgency of the situation requires it.

(5) Upon receiving the Minister's report mentioned in clause (1)(d), the Lieutenant Governor in Council, without further notice under subsection (1), may make the proposed regulation with the changes that the Lieutenant Governor in Council considers appropriate, whether or not those changes are mentioned in the Minister's report.

(6) The Minister may decide that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22 if, in the Minister's opinion, the urgency of the situation requires it.

(7) If the Minister decides that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22,

> *(a) subsections (1) to (5) do not apply to the power of the Lieutenant Governor in Council to make the regulation; and*
>
> *(b) the Minister shall give notice of the decision to the public and to the Information and Privacy Commissioner of Ontario as soon as is reasonably possible after making the decision.*

(8) The notice mentioned in clause 7(b) shall include a statement of the Minister's reasons for making the decision and all other information that the Minister considers appropriate.

(9) The Minister shall publish the notice mentioned in clause (7)(b) in The Ontario Gazette and give the notice by all other means that the Minister considers appropriate.

(10) If the Minister decides that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22 because the Minister is of the opinion that the urgency of the situation requires it, the regulation shall,

> *(a) be identified as a temporary regulation in the text of the regulation; and*
>
> *(b) unless it is revoked before its expiry, expire at a time specified in the regulation, which shall not be after the second anniversary of the day on which the regulation comes into force.*

3.1.5 Photo-comparison technology and biometric information

The announced purpose of the photo-comparison program is to reduce fraud in obtaining a driver's licence or other card.

Provisions should be transparent

Bill 85 contains provisions related to photo-comparison technology at sections 6 and 33 (complementary amendment to the *Highway Traffic Act*) at s. 32.2. These provisions should be made "transparent." We understand that the proposed technology will utilize a facial recognition software application that will convert a photograph, as has appeared for some time on our driver's licence, into a "biometric" template to allow comparisons within the Ministry's database of driver photos. Although the digital photograph the Ministry currently holds may be considered a biometric, it is the conversion of photographs into biometric templates that will allow the Ministry to perform the facial recognition comparisons.

It is essential that the government make assurances that any biometric collected, even one that has been collected for some time, only be used internally, and solely for the purpose of verifying the identity of the card holder. If the facial biometric is lost or stolen, it

cannot simply be replaced such as a PIN number. Such biometric information must be kept securely. The provisions relating to "photo-comparison technology" should be made transparent.

Recommendation 11: Given the sensitivity of biometric information, Bill 85 should be made transparent and set out that the use of biometric information be limited for internal purposes within the Ministry.

Distinguishing between biometric information and information

Currently, Bill 85 does not distinguish between "information" and "biometric information." Separating biometric information from the term "information" is important to tailor the legislation to the purpose of the Ministry's facial recognition program, which is to reduce fraud in obtaining a driver's licence or other photo card. For example, as the bill is written, biometric information could fall under the term "information" used in Bill 85's collection and disclosure provisions. Because of sections 6 and 33 in combination with s. 11(4)7 or and s. 205.0.1(4)6 (at s. 44 of Bill 85), the Minister could disclose biometric information to federal, provincial and municipal governments, and other unspecified persons or entities as prescribed, when an individual accesses benefits or services. As such, the legislation as it is written may allow for biometric information to be used as a verification procedure at all levels of government. This is clearly outside the scope of the proposed program.

Recommendation 12: "Biometric information" should be defined separate and apart from the term "information" used in Bill 85. An example of wording can be taken from the *Ontario Works Act, 1997*[6] and the *Ontario Disability Support Program Act, 1997*[7] which define "biometric information" as "information derived from an individual's unique characteristics but does not include a photographic or signature image."

Recommendation 13: In order to provide for a focused program scope and limited disclosure, Bill 85 should be amended to provide that sections 11 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1 do not apply to biometric information.

3.2 Identifying and limiting purposes

The purpose identification and limitation privacy principle requires the body collecting personal information to identify the purposes for which the information is collected and to use or disclose the information only for those purposes. In their contact with my Office on

[6] *Ontario Works Act*, 1997, S.O. 1997, c. 25, Sched. A.
[7] *Ontario Disability Support Program Act*, 1997, S.O. 1997, c. 25, Sch. B.

the EDL and the photo card for non-drivers, the Ministry informed us that legislation would be required to allow the Ministry to implement these initiatives. As noted earlier, I am not opposing the government's commitment to introduce an alternative border crossing document to the Canadian passport. I just want to make sure that privacy is built into it. It is clear from the proposed legislation that the initial purposes, that of facilitating border travel, or of facilitating everyday transactions requiring identification for those who do not or cannot drive has been expanded to include the purpose of general fraud detection in relation to government programs.

A major challenge to the principle that purposes should be clear, limited and relevant to the circumstances is the choice in Bill 85 to refer to all the above cards with one term, the "photo card." This is problematic because collection and disclosure of personal information should be directly tied to the purposes for which collection and disclosure take place. Therefore, the amount of collection or disclosure required in relation to, for example, the basic photo card will be different from the information collected or disclosed in relation to the combined photo card or enhanced photo card (alternative to a passport for travel to the U.S.). This distinction is not reflected in the bill.

3.2.1 Purposes listed in Bill 85

The purposes set out at subsections 11(4)1 to 7 and section 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)1 to 6 in Bill 85 are, respectively:

Section 11(4) 1 to 7	**Section 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)1 to 6**
(4) The only purposes for which information may be collected or disclosed under this section are the following:	(4) The only purposes for which information may be collected or disclosed under this section are the following:
1. To verify the accuracy of any information provided under this Act by an applicant for or holder of a photo card.	1. To verify the accuracy of any information provided under this Act by an applicant for or holder of a driver's licence or vehicle permit.
2. To verify the authenticity of any document provided under this Act by an applicant for or holder of a photo card.	2. To verify the authenticity of any document provided under this Act by an applicant for or holder of a driver's licence or vehicle permit.
3. To detect a false statement in any document provided under this Act by any person.	3. To detect a false statement in any document provided under this Act by any person.

4. To detect or prevent the improper use of a photo card.	4. To detect or prevent the improper use of a driver's licence or vehicle permit.
5. To detect or prevent the improper issuance or renewal of a photo card, including by conducting an audit or review of any issuance, renewal or cancellation of a photo card or the conduct of any person or entity involved in issuing, renewing or cancelling a photo card.	5. To detect or prevent the improper issuance or renewal of a driver's licence or vehicle permit, including by conducting an audit or review of any issuance, renewal or cancellation of a driver's licence or vehicle permit or the conduct of any person or entity involved in issuing, renewing or cancelling a driver's licence or vehicle permit.
6. To provide the Canada Border Services Agency or the Department of Citizenship and Immigration with information and records regarding the issuance, renewal or cancellation of an enhanced photo card or a combined photo card.	(no equivalent clause)
7. To provide a public body or related government with the information that the Minister believes is necessary to assist it with a purpose similar to a purpose set out in paragraph 1, 2, 3 or 4 if the holder of a photo card has presented his or her photo card in order to obtain a benefit or service under a legislatively authorized program or service administered or provided by that public body or related government.	6. To provide a public body or related government with the information that the Minister believes is necessary to assist it with a purpose similar to a purpose set out in paragraph 1, 2, 3 or 4 if the holder of a driver's licence or vehicle permit has presented his or her driver's licence or vehicle permit in order to obtain a benefit or service under a legislatively authorized program or service administered or provided by that public body or related government.

3.2.2 General fraud detection in relation to government programs

Subsections 11(4)7 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)6 permit any "public body" and "related governments" to obtain any information the Minister believes to be necessary to detect misuse of the cards to obtain a government benefit or service. "Public body" and "related government" are defined very broadly:

> "public body" means,
>
> > (a) any ministry, agency, board, commission, official or other body of the Government of Ontario,
> >
> > (b) any municipality in Ontario,
> >
> > (c) a local board, as defined in the *Municipal Affairs Act*, and any authority, board, commission, corporation, office or institution of persons some or all of whose members, directors or officers are appointed or chosen by or under the authority of the council of a municipality in Ontario, or
> >
> > *(d) a prescribed person or entity;* [emphasis added]
>
> "related government" means,
>
> > (a) the Government of Canada and the Crown in right of Canada, and any ministry, agency, board, commission or official of either of them, or
> >
> > (b) the government of any other province or territory of Canada and the Crown in right of any other province of Canada, and any ministry, agency, board, commission or official of any of them.

"Public body" and "related government" appears to include almost every provincial, territorial or federal department and agency in Canada, as well as unspecified entities to be prescribed by regulation, which may include private sector entities. This is because, on its face, Bill 85 does not limit the Ministry to prescribing only public authorities under subsection (d) of the definition of "public body." In fact, the description of public authorities in the definitions of "public body" and "related government" appear to be so comprehensive that the only "prescribed person or entity" that may fall within subsection (d) is a person or entity that would not otherwise be public.

Detecting and preventing fraud in the provision of benefits and services by government agencies throughout the whole of Canada is a completely different purpose from the original purpose of collecting personal information for border crossing and non-drivers for routine transactions.

In addition, because of the deeming provisions at s. 11(5) and s. 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(5), even if a disclosure does not meet the "similar purpose" requirement at ss. 11(4)7 and 44 at s. 205.0.1(4)6, the disclosure would nevertheless be deemed in compliance with *FIPPA* and *MFIPPA*.

For example, there are many situations in which, upon the presentation of a photo card, collection and disclosure may take place under ss. 11(4)7 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)6. In Ontario, people often use their driver's licence when asked for a government issued photo ID – to vote, to open a bank account or apply for a credit card, as proof of age in convenience stores or bars. The EDL and the basic and enhanced photo cards will be used in many circumstances where driver's licenses or ID cards are now required.

Combined with the wide definition of "related government" and "public body" and the lack of definitions for the terms "information" and "biometric information," Bill 85 allows for the possibility that all personal information, including an individual's biometric, driving history, citizenship data, etc., could be shared without restriction in these instances. Individuals do not reasonably expect that when applying for a library card, the provincial government will disclose their biometric, citizenship information, or other information to the library.

Another challenge to the principle that purposes should be limited and relevant to the circumstances is the proposed amendments in to the *Highway Traffic Act* regarding driver's licences and vehicle permits at s. 44 of Bill 85. It is clear that the Ministry wishes to implement a border crossing document and that it is attempting to obtain authority to do so in Bill 85. However, the bill contains virtually identical provisions to amend the *Highway Traffic Act* and will allow the same broad collection and disclosure of personal information regarding driver's licences and vehicle permits. Such broad collection and disclosure powers are for a completely different purpose not related to the original purposes described above.

Recommendation 14: Subsections 11(4)7 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)6, which allow the Ministry to widely disclose information for a purpose unrelated to the original collection when an individual presents a photo card, drivers licence, or vehicle permit in obtaining federal, provincial and municipal services and benefits, should be deleted from Bill 85.

3.2.3 Disclosure to CBSA and CIC - subsection 11(4)6

The problem posed by combining all proposed cards into the term "photo card" despite different purposes for the cards is illustrated as follows. Section 11(4)6 permits the Ministry to provide a potentially wide variety of personal information to two federal government entities for unspecified purposes. The provision permits disclosure to both the Canadian Border Services Agency (CBSA) and also to Citizenship and Immigration Canada (CIC). It is unlikely that these two departments would need the information for the same purposes. In combination with other sections in Bill 85, the lack of specificity in this section could lead to questionable scenarios.

For example, pursuant to s. 9(1)(e) the Minister may cancel a photo card if payment is rejected, such as an NSF cheque. Note, the term photo card includes a combined photo card which is in part a driver's licence. Section 4(4) states that if a driver's licence ceases to be valid for any reason, the combined photo card is also invalid. The intent of s. 11(4)6 may be to allow the Minister to notify CBSA of the invalid photo card to prevent the card from being used at the border. However, the section does not prevent the Ministry, when forwarding this information, from also including the NSF cheque, to CIC. Clearly, the purposes for collecting and disclosing information for this program are different for these two federal government entities, and Bill 85 does not reflect these differences or appropriately limit the information flow.

Recommendation 15: Subsection 11(4)6 of Bill 85 should be divided into two separate clauses, one dealing with disclosure to the Canadian Border Services Agency and one dealing with disclosure to Citizenship and Immigration Canada, and amended to specify the types of information and purposes for which the CBSA and CIC respectively may be provided with information.

Recommendation 16: Subsection 11(4)6 of Bill 85 should specify that the purposes should be limited to authentication of the cards.

3.3 Collection limitation - data minimization

The principle that the collection of personal information must be limited to only that which is necessary for specified purposes means that the amount of personal information collected must be kept to a strict minimum. This is the "data minimization" principle, and it is embodied in *FIPPA* at s. 38(2), which states no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. It has been recently affirmed at the Ontario Court of Appeal that underlying all three criteria is the requirement that

government "attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives."[8]

Bill 85 does not attempt to limit the collection of personal information to what is objectively necessary to fulfil the purposes of Bill 85. Bill 85 does not specify the classes or type of information that the Ministry may collect. Rather, subsections 11(1) and 205.0.1(1) (at s. 44 of Bill 85, complementary amendment to the *Highway Traffic Act*) provide:

> The Minister may request and collect information from any public body or related government, *as he or she considers appropriate*, *if the Minister considers it necessary* for a purpose set out in subsection (4). [emphasis added]

In contrast, Washington State's enhanced driver's licence bill (HB 1289, effective since 2007) states that the information required to be eligible for a card is specific and narrow: proof of citizenship, identity, and state residency.

The following are further examples of the potential breadth of the collection of personal information in Bill 85:

- the definition of "basic photo card" is "a card issued under this Act that has on it the holder's name and photograph *and additional information about the holder that may be prescribed*" [emphasis added];

- the definition of "enhanced photo card" is in part "a card issued under this Act that has on it the holder's name and photograph *and additional information about the holder that may be prescribed…*" [emphasis added];

- section 3(1)(d) states that after the phasing-in period, the Minister may issue a basic photo card to an individual who "meets *any other requirements that may be prescribed*" [emphasis added];

- section 3(2)(e) states that after the phasing-in period, the Minister may issue an enhanced photo card to an individual who "meets *any other requirements that may be prescribed*" [emphasis added];

- section 22 (b) provides that regulations may be made prescribing additional information about the holder that may be included on a basic photo card, enhanced photo card or combined photo card.

Personal information collected by the Ministry should be limited to that which is objectively necessary and related to eligibility for a card. Although we understand that it is

[8] *Cash Converters Canada Inc. v. Oshawa (City)* [2007] O.J. No. 2613 at 30 and 31.

not the Ministry's intent, we illustrate that as written, Bill 85 could lead to the alarming possibility of basic, enhanced and combined photo cards containing, for example, race, religion, sexual orientation, marital status or blood type information.

We prefer that the government list in the statute itself the types and classes of personal information to be collected in support of this. We note that the personal information required to be submitted in a passport application has not changed significantly over time. Also, other provinces that have a basic photo card in place have identified the specific data fields required for the collection of personal information. For example, New Brunswick's *Motor Vehicle Act*, R.S.N.B. 1973, c. M-17 states "85(2) Every application shall state the full name, date of birth, sex, and resident address of the applicant…."

Furthermore, since the basic photo card is not a licence and will not be used for crossing the U.S. border, data minimization should be applied regarding the amount of personal information collected for that card. In other words, it should not be assumed that the same amount of personal information is required to issue a basic photo card as is required for a driver's licence, or an enhanced or combined photo card. In theory, there should be less personal information collected since the card is not imparting duties which are enforced by the government, such as driving safely. This is a further example of the problem posed by combining all cards within the term "photo card."

Data minimization concerns also arise from Bill 85's amendment of Part XIV of the *Highway Traffic Act* (see s. 44 of Bill 85 at s. 205.0.1) to permit a wide variety of collections of information by the Ministry and disclosures of information by the Ministry to a "related government" or "public body," which is very widely defined. Consider that Part XIV of the *Highway Traffic Act* alone deals with a variety of reports and documents, many of which may contain personal information, including:

- accident reports made to police by individuals involved in a motor vehicle accident;
- notices by insurers and other prescribed persons to the Registrar of Motor Vehicles and the owner of the vehicle that a vehicle involved in an accident is irreparable;
- information provided to the police by a driver who has been in an accident (name, driver's licence number, insurance policy number, name and address of vehicle owner and vehicle permit number);
- reports to the Registrar by doctors if patients are suffering from a condition that would make it dangerous for them to drive;
- reports from optometrists who have patients that cannot see well enough to drive; and
- an operating record for every driver showing all reported convictions for driving offences and all reported unsatisfied judgments against the driver.

Bill 85's lack of data minimization is even more of a concern when one realizes that Bill 85 allows the Ministry to potentially disclose all collected personal information to a wide variety of federal, provincial and municipal government bodies and possibly private individuals and companies, including unspecified persons and entities to be prescribed by

regulation. Moreover, as described under the heading "Use and disclosure limitation" below, the Ministry can disclose personal information for purposes that may be only peripherally related, if at all, to the original purposes for which this information was collected.

Recommendation 17: The types of information to be collected, used or disclosed by government authorities under Bill 85 must be specified in the bill itself.

Recommendation 18: Sections 11(1) and (3) of Bill 85 should be amended to provide that only collections, uses, and disclosures that are objectively necessary to accomplish the purposes set out in the section are permitted.

3.4 Use and disclosure limitation

3.4.1 Minister to subjectively decide how much personal information

As stated earlier, the principle of use and disclosure limitation requires that personal information shall not be used or disclosed for purposes other than the purposes for which it was collected, except with the consent of the individual or as required by law.

Bill 85 does not limit the use and disclosure of personal information to the purposes for which the information was collected. Bill 85 allows any public body to decide subjectively what information may assist the Minister and disclose it to him or her. It also allows the Ministry to disclose to any public body or related government any information the Ministry considers appropriate and subjectively believes necessary to assist. Subsections 11(2), (3) and (4)7 of the bill provide:

> *11. (2) The Minister may disclose information to any public body or related government, as he or she considers appropriate, if the Minister considers it necessary for a purpose set out in subsection (4)*
>
> *(3) Upon receipt of a request for information from the Minister under subsection (1), a public body shall disclose to the Minister any information from their records that may assist the Minister with a purpose set out in subsection (4).*
>
> *(4) The only purposes for which information may be collected or disclosed under this section are the following:*
>
> *7. To provide a public body or related government with the information that the Minister believes is necessary to assist it with a purpose similar to a purpose set out in paragraph 1, 2, 3 or 4 if the holder of a photo card has presented his or her photo card in order to obtain a benefit or service under a*

legislatively authorized program or service administered or provided by that public body or related government.

These provisions give the Ministry and public bodies and related governments overly broad discretion to disclose personal information to each other. As recommended under the heading "Collection limitation – data minimization," the types and classes of personal information to be collected should be explicitly described.

Recommendation 19: Sections 11 and 44 (complementary amendment to the *Highway Traffic Act)* at s. 205.0.1 of Bill 85 should be amended to provide that the use and disclosure of personal information by the Ministry and by public bodies and related governments must be limited to that which is objectively necessary and for the purposes for which it was collected, namely, establishing eligibility for each of the photo cards.

3.4.2 Complementary amendments to the *Highway Traffic Act*

Further use and disclosure limitation concerns arise from Bill 85's complementary amendment of Part XIV of the *Highway Traffic Act* to permit a wide variety of collections and disclosures of information by the Ministry to and from a related government and public body, which is very widely defined and allows for disclosure to unspecified persons and entities.

The broad authority in Bill 85, in combination with the deeming provision, could allow disclosures to entities that should not have access to Ontario drivers' personal information, such as the driver's or vehicle owner's address.

Recommendation 20: Section 44 of Bill 85 should be amended to provide that the use and disclosure of personal information by the Ministry and by public bodies and related governments must be limited to that which is objectively necessary and for the purposes for which it was collected, namely, establishing eligibility for a driver's licence or vehicle permit.

4. Conclusion

As we have stated, we are not opposed to the Ministry's initiatives, but we have concerns regarding privacy, which should, and can, be addressed with our continued collaborative efforts. Thank you for this opportunity to provide comment on the *Photo Card Act, 2008*.

5. List of Recommendations

1. The Ontario government must strongly pursue the federal government to take responsibility for verifying the citizenship status of naturalized Canadian citizens and providing that information to Ontario for the purpose of the Enhanced Driver's Licence and Enhanced Photo Card. Ontario cannot create a new collection and retention of personal information already existing in the hands of the federal government. The principle of data minimization must be observed.

2. To assure the Canadian public of the government's commitment to protecting their personal information and identity when implementing an RFID technology system, there must be an independent privacy audit and end-to-end threat risk assessment that adequately identifies and addresses any privacy and security issues.

3. Any use of RFID technology by the Ontario government must comply with the RFID guidelines developed by the Office of the Information and Privacy Commissioner of Ontario.

4. The Ministry must work with a selected vendor to pursue adding a privacy-enhancing on/off switch for the RFID tag embedded in the card.

5. Bill 85 should be amended with language similar to Sections 39 and 42 of *PHIPA* to require that any authorized disclosure of personal information to other Ontario institutions not covered by *FIPPA* and *MFIPPA*, other territorial or provincial governments, the Government of Canada, or any agency of the Government of the United States, only be made subject to an appropriate agreement that safeguards the personal information.

6. Bill 85 should set out the minimum contents of such disclosure agreements. For example, the agreements must provide for transferring the minimum amount of information (otherwise known as data minimization), and for monitoring and auditing of compliance. Except to the extent of legitimate security needs for the confidentiality of certain clauses, the full agreements should be made readily available to the public.

7. Bill 85 should be amended to delete subsections 11(5) and 205.0.1(5) (contained at s. 44 of Bill 85) so that sections 42 of *FIPPA* and 32 of *MFIPPA* will apply to disclosures of information.

8. Subsection 21(2) of Bill 85 should be amended to include a standard of good faith.

9. Bill 85 should be amended to add a subsection (3) to s. 21 that mirrors the wording of 5.4(2) at s. 29 (amendment to the *Highway Traffic Act*).

10. Bill 85 should be amended to provide for public consultation before regulations are promulgated as follows:

(1) Subject to subsection (7), the Lieutenant Governor in Council shall not make any regulation under section 22 unless,

(a) the Minister has published a notice of the proposed regulation in The Ontario Gazette and given notice of the proposed regulation by all other means that the Minister considers appropriate for the purpose of providing notice to the persons who may be affected by the proposed regulation;

(b) the notice complies with the requirements of this section;

(c) the time periods specified in the notice, during which members of the public may exercise a right described in clause (2)(b) or (c), have expired; and

(d) the Minister has considered whatever comments and submissions that members of the public have made on the proposed regulation in accordance with clause (2)(b) or (c) and has reported to the Lieutenant Governor in Council on what, if any, changes to the proposed regulation the Minister considers appropriate.

(2) The notice mentioned in clause (1)(a) shall contain,

(a) a description of the proposed regulation and the text of it;

(b) a statement of the time period during which members of the public may submit written comments on the proposed regulation to the Minister and the manner in which and the address to which the comments must be submitted;

(c) a description of whatever other rights, in addition to the right described in clause (b), that members of the public have to make submissions on the proposed regulation and the manner in which and the time period during which those rights must be exercised;

(d) a statement of where and when members of the public may review written information about the proposed regulation;

(e) all prescribed information; and

(f) all other information that the Minister considers appropriate.

(3) The time period mentioned in clauses (2)(b) and (c) shall be at least 60 days after the Minister gives the notice mentioned in clause (1)(a) unless the Minister shortens the time period in accordance with subsection (4).

(4) The Minister may shorten the time period if, in the Minister's opinion, the urgency of the situation requires it.

(5) Upon receiving the Minister's report mentioned in clause (1)(d), the Lieutenant Governor in Council, without further notice under subsection (1), may make the proposed regulation with the changes that the Lieutenant Governor in Council considers appropriate, whether or not those changes are mentioned in the Minister's report.

(6) The Minister may decide that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22 if, in the Minister's opinion, the urgency of the situation requires it.

(7) If the Minister decides that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22,

> *(a) subsections (1) to (5) do not apply to the power of the Lieutenant Governor in Council to make the regulation; and*
>
> *(b) the Minister shall give notice of the decision to the public and to the Information and Privacy Commissioner of Ontario as soon as is reasonably possible after making the decision.*

(8) The notice mentioned in clause 7(b) shall include a statement of the Minister's reasons for making the decision and all other information that the Minister considers appropriate.

(9) The Minister shall publish the notice mentioned in clause (7)(b) in The Ontario Gazette and give the notice by all other means that the Minister considers appropriate.

(10) If the Minister decides that subsections (1) to (5) should not apply to the power of the Lieutenant Governor in Council to make a regulation under section 22 because the Minister is of the opinion that the urgency of the situation requires it, the regulation shall,

> *(a) be identified as a temporary regulation in the text of the regulation; and*
>
> *(b) unless it is revoked before its expiry, expire at a time specified in the regulation, which shall not be after the second anniversary of the day on which the regulation comes into force.*

11. Given the sensitivity of biometric information, Bill 85 should be made transparent and set out that the use of biometric information be limited for internal purposes within the Ministry.

12. "Biometric information" should be defined separate and apart from the term "information" used in Bill 85. An example of wording can be taken from the *Ontario Works Act, 1997* and the *Ontario Disability Support Program Act, 1997* which define "biometric information" as "information derived from an individual's unique characteristics but does not include a photographic or signature image."

13. In order to provide for a focused program scope and limited disclosure, Bill 85 should be amended to provide that sections 11 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1 do not apply to biometric information.

14. Subsections 11(4)7 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1(4)6, which allow the Ministry to widely disclose information for a purpose unrelated to the original collection when an individual presents a photo card, drivers licence, or vehicle permit in obtaining federal, provincial and municipal services and benefits, should be deleted from Bill 85.

15. Subsection 11(4)6 of Bill 85 should be divided into two separate clauses, one dealing with disclosure to the Canadian Border Services Agency and one dealing with disclosure to Citizenship and Immigration Canada, and amended to specify the types of information and purposes for which the CBSA and CIC respectively may be provided with information.

16. Subsection 11(4)6 of Bill 85 should specify that the purposes should be limited to authentication of the cards.

17. The types of information to be collected, used or disclosed by government authorities under Bill 85 must be specified in the bill itself.

18. Sections 11(1) and (3) of Bill 85 should be amended to provide that only collections, uses, and disclosures that are objectively necessary to accomplish the purposes set out in the section are permitted.

19. Sections 11 and 44 (complementary amendment to the *Highway Traffic Act*) at s. 205.0.1 of Bill 85 should be amended to provide that the use and disclosure of personal information by the Ministry and by public bodies and related governments must be limited to that which is objectively necessary and for the purposes for which it was collected, namely, establishing eligibility for each of the photo cards.

20. Section 44 of Bill 85 should be amended to provide that the use and disclosure of personal information by the Ministry and by public bodies and related governments must be limited to that which is objectively necessary and for the purposes for which it was collected, namely, establishing eligibility for a driver's licence or vehicle permit.