EDL Speaking Notes to the Standing Committee on General Government, regarding Bill 85, *Photo Card Act, 2008*

Introduction

I would like to begin by thanking members of the Standing Committee on General Government for the opportunity to make a presentation today during its review of Bill 85, commonly referred to as the *Photo Card Act, 2008*.

As Ontario's Information and Privacy Commissioner, my mandate encompasses many responsibilities. Of these, I believe that providing counsel on the privacy implications of proposed legislation or sweeping technological changes to government is one of my most important duties. I also believe it is vitally important to be practical in the protection of privacy, and ensure that the right information reaches the public. Unless the public is informed of what the privacy issues are – and the associated concerns – these issues may surface only after the fact, when it may be too late. The public needs to understand the implications of this new program and legislation in order to make an informed choice if they decide to apply for one of these cards.

The primary purpose behind this proposed Bill is to enable the government to issue an enhanced driver's licence, which I'll refer to as an EDL, which are intended to serve as an alternative to a passport, solely for the purposes of entering the United States. In addition, the Bill 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 visual impairment. Such photo cards are available in virtually all other provinces. Bill 85 makes these available in Ontario and also allows the government to enhance them to serve as an alternative to a passport, when travelling to the United States—parallel to an EDL.

I further understand that the entire Western Hemisphere Travel Initiative, which I will refer to, as it is commonly called — as WHTI, has grown out of security concerns following the events of 9/11. As an individual citizen, I certainly understand peoples' fears relating to terrorism. However, as Commissioner, I also fear the potential loss of our freedoms, especially over privacy, which forms the basis of <u>all</u> of our freedoms.

In the days and months following 9/11, many people, especially those in the United States, were hesitant to speak out on behalf of privacy for fear of it being viewed as being unpatriotic. I remember vividly, days after 9/11, in response to a call from the CBC seeking my "position" on the event, I issued a position paper posted jointly to our websites, headed: *Public safety is paramount, but balanced against privacy*. The position I took was that, of course, we had to protect public safety but, and a very important "but," we also had to ensure that any security measures undertaken were real and not illusory. They had to be necessary and effective. We couldn't just give up our privacy, our freedom, for the mere *appearance* of security – it had to be real. I argued that our search for safety and security could not come at the expense of privacy. This would be a fundamental error. Forfeiting our privacy in the pursuit of security is simply too high a price to pay. Since, privacy is at the heart of freedom.

Having said that, I want to make clear that my purpose here today is not to oppose Bill 85, but rather to share some concerns I have with the legislation. I also want to state for the record, that I am not opposing the government's commitment to introduce an alternative border crossing document to the Canadian passport. I will remind you how this came about and is actually the lesser of two evils. I just want to make sure that privacy is built into the program.

Let me first tell you that over the last year, my office has developed a good working relationship with the Ministry of Transportation (MTO), and Ontario's Intergovernmental Affairs and Cabinet Office, who have been keeping my office informed of the implications of WHTI and Ontario's plans to implement an alternative border crossing device acceptable to the U.S. government.

My office has been proactive in advancing the public's understanding of this project. This past summer, I had the opportunity to jointly co-host, with Professor Andrew Clement, of the University of Toronto, a public forum on the privacy and security issues involving the EDL. We heard arguments from members of both sides of the debate, including from the University of Toronto's, Identity, Privacy and Security Initiative, an excellent program, as well as representatives from both the provincial and federal governments, and consumer and citizen interest groups such as the Consumer Council of Canada, the Binational Tourism Alliance, and the Canadian National Institute for the Blind. This multi-stakeholder input was very helpful in clarifying various elements of the EDL program.

Moving forward, I would now like to give you an overview of my privacy concerns regarding Bill 85.

After careful study, we noticed that Bill 85 was missing several privacy principles commonly included under internationally recognized Fair Information Principles. While each of these principles is detailed in my submission, I will discuss just one here, that speaks to the question of "accountability."

Accountability – Openness and Transparency/Public Consultation

Openness and transparency are key to government accountability, especially when the government serves as the custodian of a significant amount of personal information on its citizens. My concern here is that 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 are not defined in Bill 85 and do not list the specific personal information to be collected, used or disclosed by the government or details, such as:

- The information to be contained on the photo card;
- The security and other features that may allow the photo card to be used for travel purposes;

- The information that the Ontario government will collect from municipalities and other provincial, territorial and federal government departments and agencies, which is too broad;

- The information that the Ontario government will provide to municipalities and other provincial and federal government departments and agencies, is not clear;

- The contents of information-sharing agreements; and

- The requirements for being issued a photo card.

Under these circumstances, in order for transparency and accountability to be achieved, the regulation-making powers provided for under Bill 85 must allow for public consultation before a regulation is enacted. This would not be the first time in Ontario that such consultation was set out in legislation. Other instances include the *Personal Health Information Protection Act*, the *Environmental Bill of Rights*, and the *Occupational Health and Safety Act*.

As government officials and public servants, I feel that we must provide an opportunity for the people of Ontario to voice their thoughts and views regarding a decision that may impact their lives In my recommendations, I have suggested specific wording to accomplish this based on the wording contained in Ontario's *Personal Health Information Protection Act.*

With regards to government accountability, I would also like to state that Bill 85's provisions relating to photo-comparison technology should be made more "transparent." It is my understanding that the proposed technology will utilize a facial recognition software application that will convert a photograph, as has appeared on our driver's licence for many years, into a biometric template, to allow comparisons within the Ministry's database of driver photos. The government must make assurances that any biometric collected, even one that the public is accustomed to and that has been collected for some time, will only be used internally, and solely for the purpose of verifying the identity of card holders. Placing strict controls on its use is crucial.

In the remaining time, I am going to devote my comments to two important areas: verification of citizenship information, and Radio Frequency Identification technology or RFIDs. First, let me briefly discuss the issue of citizenship verification.

Citizenship Verification/Duplication of Databases

Earlier this year, I went so far as issuing a press release to make the public aware of one of my biggest concerns regarding the security risks associated with the proposed EDL program. Provinces are being asked to verify the citizenship of applicants for the purpose of the EDL program (and the enhanced photo card for non-drivers). Applicants will have to provide proof of Canadian citizenship to the Ministry of Transportation, complete a questionnaire (with questions such as "At the time of your birth, was one of your parents a foreign diplomat, consular officer or

representative or employee of a foreign government recognized by the Canadian Government?" "Did one of your parents ever renounce or give up their Canadian citizenship before February 15, 1977?"), and undergo an in-person interview.

I respectfully asked that the federal government - the Government of Canada, securely provide citizenship information on naturalized citizens (those not born in Canada), to Ontario to avoid the need to recreate a duplicate process of verifying citizenship for Canadians who apply for an EDL.

This isn't something new. We have several precedents – other examples of secure information sharing between our federal and provincial governments. For example:

- Ontario's GAINs program, which receives tax status information on individuals from the federal Canada Revenue Agency, who possesses that information;

I initiated a dialogue with The Honourable Stockwell Day, Minister of Public Safety, responsible for national coordination of the EDL program, some time ago, to request that the Department of Citizenship and Immigration (CIC) provide the citizenship information they hold to provinces that request it.

Further, in early correspondence with Ontario's Deputy Minister of Transportation and the Deputy Minister of Intergovernmental Affairs, I noted the fact that when it comes to responsible information management, the practice of data minimization should always prevail, meaning, don't collect any new information — new personal data — if you don't have to. Requiring provinces to build their own database of citizenship information from scratch – in effect, re-inventing the wheel, when the federal government already has this information – 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 time and resources, not to mention our taxpayer dollars, by duplicating existing government resources.

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 information. And lest you think that this is a simple "yes-no" answer for citizenship, I assure you, it is not. The database would apparently need to contain the answers and notes to a lengthy in-person interview for each applicant. And it may not end there. If the interview questions reveal a complicated situation, the matter is then to be forwarded to the Federal government in any an event, resulting in further duplication, cost and privacy risk. This is no simple matter. Let's not complicate it further.

And let me be clear – I know this is a federal issue, not the doing of the Premier or Minister of Transportation. But regardless of the fact that it was created by the federal government, it must be resolved now. The Federal government already has this information. It 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 is clearly a more privacy protective and cost effective model – a "win/win" scenario – more privacy and security; lower cost.

Now, let me turn to another area which I feel is a very critical aspect of Bill 85 – the use of Radio Frequency Identification technology or RFIDs.

RFID Technology

For those of you who may not be familiar with RFID technology, let me give you very a brief introduction to the topic, and I mean brief.

RFID is a generic term for a variety of technologies that use radio waves for purposes of automatic identification, consisting of two integral parts: a tag, and a reader – think "bar code on steroids."

There are two main types of RFID tag: active or passive, which differ depending on whether they have their own power system. Passive tags have no power source and no on-tag transmitter.

Finally, you need to know that RFID tags are activated by readers, which, in turn, are connected to a host computer. In a passive system, the RFID reader transmits a signal via the airwaves that "wakes up" the tag by powering up its chip, which in turn enables it to transmit data.

I have spent many years working in this field, trying to secure privacy within RFID technology, and my Office has produced three papers and a set of practical guidelines on the subject. I am not opposed to the use of RFID tags across the board – indeed, they can have many benefits. But, like all information technologies, they need to have privacy issues baked in to them early in the design of these systems. I call this "privacy by design," a term I first developed in the early 90s, which ensures that privacy does not become an afterthought, because is has been built right into the system.

Tagging things in areas such as the supply-chain management process or taking an inventory of assets, posses no risk to privacy. *Tagging Things Linked to People*, however, can raise concerns because of the relative permanence of the tag, the nature and amount of data collected, and the strength of the data's linkage to personally identifiable individuals, in addition to the sensitivity of the data involved. Once you have the possibility of data linkage, allowing for individuals to become identifiable, that's when privacy concerns arise.

Here's how this relates to Bill 85 and the EDL program:

Currently, U.S. Customs and Border Protection (CBP) uses RFID technology on its trusted or registered traveler programs – such as NEXUS - 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." The Department of Homeland Security requires that any approved border travel document carry RFID tags.

Arlene White, Executive Director for the Bi-national 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 we held, about these border communities and their strong support for this program. She emphasized their desire to ensure the smooth flow of traffic at their borders which, in her view, would not be possible without this RFID technology.

Let me now give you some sense of what all of this means with regards to privacy and security.

A fundamental characteristic of all RFID technologies is that they are wireless. This means that any data contained on the chip – in this case, a unique index number which is stored on the embedded RFID chip – is transmitted through an RFID reader to a database of information. This number serves as a pointer to the individual's personal information contained in the database, needed for the completion of this process.

Now, there are well-known privacy and security vulnerabilities associated with RFID technology that are commonplace, and apply to <u>any</u> RFID-enabled identification card and information system. Briefly, the top three are:

- **Skimming** – which occurs when an individual with an unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge; Remember, the RFID is emitting radio frequencies that can be picked up by any readers in the area, authorized or unauthorized;

- **Eavesdropping** – which occurs when an unauthorized individual intercepts data, using an authorized RFID reader;

- **Cloning** – which occurs when the unique information contained on the original RFID chip is read or intercepted, and its data are duplicated.

These vulnerabilities could lead to a host of undesirable consequences such as unauthorized identification, identity theft and most serious, the surreptitious tracking and surveillance of individuals – say good-bye to privacy.

In response to some of these concerns, you will be told that the RFID Gen2 standard, to be used for the EDL, does not include any personally identifiable information, only a unique number linking the cardholder to his or her record in a database, so no privacy concerns, right? **WRONG!** Just think of a social insurance number, a passport number or a driver's licence number – while each of these 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 subject to abuse, by unauthorized parties or used for unintended purposes that may cause real harm to real people. Just think of identity theft as a case in point.

So a number, when uniquely linked to an individual, is <u>not</u> inconsequential – it's not just a meaningless number – it points to real, personally identifiable information, that may then be subjected to abuse.

Regardless of the contents of the data stored on the chip, if that data is both static 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, it could be used to collect information in the future. I know this sounds like wildly futuristic scenarios, but I assure you, it's not that far off.

In the here and now, Identity Theft 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 – much of which is due to organized crime having entered into the scene, en mass.

Currently, the suggested method for allowing cardholders a measure of privacy and security is to provide them with an "electronically opaque" sleeve, called a Faraday Cage, which would prevent communications to and from the RFID chip, if the card was encased in the sleeve – some call it the Dorito Chips bag – aluminum foil also does the trick.

But this is **not** a sufficient answer. The cardholder must take on an added inconvenience, but must also remember to place his or her card into such a device. It won't happen. They won't remember to do it, or bother to do it, or want to do it. They'll want the ease of slipping their licence into their wallets, just like they do now.

This proposed protective sleeve, when offered as the only privacy measure, would realistically 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 sleeve. This solution is only protective when the individual remembers to place the card in the sleeve – otherwise, the reading of cards becomes free and clear.

Even leading researchers such as Sophia Cope, staff attorney and a fellow at the Center for Democracy and Technology 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, Ms. Cope stated that privacy risk mitigation measures such as the Faraday sleeve, ***"improperly place the burden of privacy protection on the citizen. Moreover, they offer no protection in light of the fact that the EDL 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.

As the RFID standard chosen for this project will respond to any reader query, I feel that the card must have some means of preventing it from being read when not required, when used for multiple purposes other than border crossing – a better solution than the proposed sleeve is needed.

So the way that I always proceed is to go off and look for solutions. One of the best options that I've heard of would be to give the cardholder the option of physically verifying the selected

transmission setting, meaning adding the equivalent of an "on/off" switch to the RFID, which can be incorporated directly onto the card.

And I am not proposing this based on "yet-to-be-developed" technology. Several groups are developing this. At MIT, The Media Lab has already patented and prototyped an "on/off switch" for the RFID tag that can be incorporated directly into a card, allowing the card holder to determine when and where their information will be transmitted.

So has another company based in the U.K. – Peratech, a company that has advanced this even further, having developed an on/off switch using Quantum Tunneling Composites technology. Its founder and CTO David Lussey advised me 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 used by all the major RFID card manufacturers. And it is just a matter of cents, not dollars, that we are talking about."*** This is indeed a very promising prospect.

There's also another company in the United States – Root Labs -- which is working on a similar switch that will be placed on transponders used by San Francisco Bay highway toll users.

I brought together our government and the vendor selected to produce EDLs in Ontario, hoping to advance this very promising technology, that I believe should be seriously considered for EDLs here in Ontario. I felt that it was necessary to bring them together, with the goal of advancing the feasibility and development of this promising technology. In fact, a senior executive, from the government's selected vendor, told me, ***"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 third-party technologies to enhance RFID functionality, security and also privacy."***

Great – the more options available, the better. Stay tuned.

<u>Privacy by Design</u>

Let me shift gears now and give you some perspective, by way of background, on privacy and technology. Since the early 90s, I have been advancing the idea that technology has the ability, not only to provide good security; it also has the ability to protect our privacy. In 1995, I put forward the view that technology can liberate us from the "zero-sum" trap of having to sacrifice privacy in order to have security. But in order to do this, we have to move forward toward a "positive-sum" paradigm. We cannot view privacy and security as polar opposites. In this new positive sum "win-win" scenario, privacy and security can <u>both</u> co-exist because technology is enlisted to protect privacy and safeguard personal information through the use of privacy-enhancing technologies (PETs). When applied to technologies of surveillance, PETs can serve to transform these technologies into ones that are protective of privacy, hence my new term, "transformative technologies." I say transformative technologies because I believe that technology has evolved to the point where it now has the ability to protect our privacy while

performing whatever functionality it was designed to perform, but only if privacy is built directly into the architecture of that technology at the developmental stage. As I've said, I call this "privacy by design," and it is my mantra. Privacy can either be achieved through the use of PETs, by eliminating or minimizing the collection of personal data, or by preventing the unnecessary and undesirable uses of personal data, all without losing the functionality of that technology. And this can be achieved by keeping privacy in mind and embedding it into the design and architecture of new technologies – Win/Win, not either/or!

And so, in the spirit of the above, I recommend the following regarding the use of RFID technology, in the EDL.

First, I would like to recommend that any use of Radio Frequency Identification technology comply with the RFID guidelines set by my office (and I have brought along a copy with me today, for your convenience.)

Second, and most important, I recommend that the Ministry work with the selected vendor to pilot test the privacy-enhancing technology of adding an on/off switch for the RFID tag embedded in the card. This will enable far greater protection of the card, when not being used for border-crossing purposes.

Conclusion

Let me conclude by sharing a motto that my office developed some time ago, and follows religiously. I call it the 3C's: Consultation; Collaboration; and Co-operation. This philosophy, I believe, represents the ethos of my office and this is the attitude I carry into my work regarding the EDL program.

As I have stated, I am not opposed to the EDL program, but I do have concerns regarding privacy, which I feel must be addressed, based on the mandate given to me by the Legislature of Ontario – and I look forward to serving that mandate in the spirit of the 3 C's.

Thank you once again for providing me with the opportunity to appear before the Committee and for considering my Office's comments on the *Act*. I am confident that, with our continued collaborative efforts, we will be able to appropriately address any outstanding privacy matters and to best serve the people of Ontario. In fact, we could develop the most privacy protective EDL available, anywhere in the world – another first for Ontario, and hopefully, one of many more to come.

Thank you.