G-11

ISSN 1180-5218

Legislative Assembly of Ontario

First Session, 39th Parliament

Assemblée législative de l'Ontario

Première session, 39e législature

Official Report of Debates (Hansard)

Monday 20 October 2008

Journal des débats (Hansard)

Lundi 20 octobre 2008

Standing Committee on General Government

Comité permanent des affaires gouvernementales

Photo Card Act, 2008

Loi de 2008 sur les cartes-photo

Chair: Linda Jeffrey
Clerk: Trevor Day

Présidente : Linda Jeffrey
Greffier : Trevor Day

Hansard on the Internet

Hansard and other documents of the Legislative Assembly can be on your personal computer within hours after each sitting. The address is:

Le Journal des débats sur Internet

L'adresse pour faire paraître sur votre ordinateur personnel le Journal et d'autres documents de l'Assemblée législative en quelques heures seulement après la séance est :

http://www.ontla.on.ca/

Index inquiries

Reference to a cumulative index of previous issues may be obtained by calling the Hansard Reporting Service indexing staff at 416-325-7410 or 325-3708.

Renseignements sur l'index

Adressez vos questions portant sur des numéros précédents du Journal des débats au personnel de l'index, qui vous fourniront des références aux pages dans l'index cumulatif, en composant le 416-325-7410 ou le 325-3708.

Hansard Reporting and Interpretation Services
Room 500, West Wing, Legislative Building
111 Wellesley Street West, Queen's Park
Toronto ON M7A 1A2
Telephone 416-325-7400; fax 416-325-7430
Published by the Legislative Assembly of Ontario

Service du Journal des débats et d'interprétation
Salle 500, aile ouest, Édifice du Parlement
111, rue Wellesley ouest, Queen's Park
Toronto ON M7A 1A2
Téléphone, 416-325-7400; télécopieur, 416-325-7430
Publié par l'Assemblée législative de l'Ontario

LEGISLATIVE ASSEMBLY OF ONTARIO

ASSEMBLÉE LÉGISLATIVE DE L'ONTARIO

STANDING COMMITTEE ON GENERAL GOVERNMENT

COMITÉ PERMANENT DES AFFAIRES GOUVERNEMENTALES

Monday 20 October 2008

Lundi 20 octobre 2008

The committee met at 1402 in room 228.

SUBCOMMITTEE REPORT

The Vice-Chair (Mr. David Orazietti): Good afternoon, everyone. We'll get started. We are here this afternoon to consider deputations 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.

I understand there's a subcommittee report. Ms. Mitchell.

Mrs. Carol Mitchell: Your subcommittee met on Tuesday, September 23 to consider the method of proceeding 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, and recommends the following:

(1) That the committee meet in Toronto on Wednesday, October 15, 2008 and Monday, October 20, 2008, for the purpose of holding public hearings.

(2) That the committee clerk, with the authorization of the Chair, post information regarding public hearings in local newspapers in the border communities of Kingston, Niagara, Sarnia, Sault Ste. Marie, and Windsor, as well as the Globe and Mail and L'Express for one day during the week of September 29, 2008. This is to include French newspapers where applicable.

(3) That the committee clerk, with the authorization of the Chair, post information regarding public hearings on the Ontario parliamentary channel and the Legislative Assembly website.

(4) That interested parties who wish to be considered to make an oral presentation contact the committee clerk by 12 noon on Friday, October 3, 2008.

(5) That groups and individuals be offered 10 minutes for their presentation. This time is to be scheduled in 15-minute increments to allow for questions from the committee.

(6) That, in the event all witnesses cannot be scheduled, the subcommittee consider an additional day of public hearings.

(7) That the research officer provide the committee with the requested background information by Thursday, October 9, 2008.

(8) That the Minister of Transportation be invited to appear before the committee to make a presentation of up to 15 minutes followed by 15 minutes of questions by the committee.

(9) That the Information and Privacy Commissioner be invited to appear before the committee to make a presentation of up to one hour. This time would include questions from committee members.

(10) That the deadline for written submissions be 5 p.m. on Monday, October 20, 2008.

(11) That the research officer provide the committee with a summary of presentations prior to 12 noon on Wednesday, October 22, 2008.

(12) That for administrative purposes, proposed amendments be filed with the committee clerk by 5 p.m. on Thursday, October 23, 2008.

(13) That the committee meet for the purpose of clause-by-clause consideration of the bill on Monday, October 27, 2008.

(14) That the committee clerk, in consultation with the Chair, be authorized prior to the adoption of the report of the subcommittee to commence making any preliminary arrangements necessary to facilitate the committee's proceedings.

Mr. Chair, both days will not be required as we were able to meet all of the requests in one day of appearances.

The Vice-Chair (Mr. David Orazietti): Thank you for that, Ms. Mitchell. Any debate? Seeing none, all in favour? Opposed? Carried.

PHOTO CARD ACT, 2008

LOI DE 2008 SUR LES CARTES-PHOTO

Consideration of 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 / Projet de loi 85, Loi permettant la délivrance de cartes-photo aux résidents de l'Ontario et apportant des modifications complémentaires au Code de la route.

STATEMENT BY MINISTER AND RESPONSES

The Vice-Chair (Mr. David Orazietti): For our next item, we have a presentation from the Honourable Jim Bradley, the Minister of Transportation. Would he like to come forward with any staff that perhaps are with him for the presentation? I understand the presentation will be

about 15 minutes, and I'll allow 15 minutes for questions, which will be five minutes for each caucus. Whenever you're ready.

Hon. James J. Bradley: Good afternoon, members of the committee. Thank you for inviting me to be with you today. I'm with Sam Erry and Steve Burnett from the ministry. I think we have as well legal counsels Patrick Moore and Todd Milton, senior business adviser Catherine Brooks—they're in the room behind us, so we're with you today. Gilles Bisson asked that we pause a moment until he's able to come back.

Mr. Gilles Bisson: I'm back.

Hon. James J. Bradley: He's back. So I wanted to accommodate his wishes.

I'm here today to tell you about several important steps in our government's plan to keep our economy moving and build a safe and prosperous Ontario. The first part of the plan is to provide Ontarians with a convenient and secure passport alternative for use at Canada-US land and sea border crossings. Next, we plan to implement a much-needed technology that will help ensure the integrity and security of these cards. Finally, to improve access and opportunity for all, we are proposing a completely new card, a photo identification card for Ontarians who do not drive.

Of course, these new cards will provide options for Ontarians. Obtaining them will be completely voluntary. As many of you are aware, the US government started implementing the western hemisphere travel initiative as a key recommendation of the 9/11 commission report. As of June 1, 2009, travellers entering the US by land or sea will be required to present a passport or an acceptable alternative. That is why this government has proposed that a new, enhanced version of the existing Ontario driver's licence be available as an alternative.

With about half of all Canadians holding a passport, we want to make it as simple as possible for Ontario travellers to access a secure border-crossing document. This is a great opportunity for the province to take a leadership role in supporting our economy by helping to avoid confusion and traffic congestion at the border. I think we would all agree, particularly those who represent border areas but those who are not far from the border as well, that this is an enviable goal which I think is shared, if I may say so, by individuals and elected representatives on both sides of the border—along the northern United States and the southern part of Canada, not only our province, but others. We wish to minimize delay for travellers and commercial drivers as a result of the new US requirements. This new secure driver's licence card would offer the same privileges as the existing card, with the addition of information needed to show proof of Canadian citizenship. That is what is looked for at the borders: the proof of your citizenship at the time when the full impact of the United States requirements and Canadian requirements are in effect. The new secure photo card would extend this border crossing advantage to Ontarians who do not hold a driver's licence. Our borders are the economic gateway to this province and must remain safe, open and accessible on June 1, 2009, and indeed every day. Our economy and our prosperity depend on it.

I was Minister of Tourism for a period of about four years and I recognized in that portfolio in particular—though those who have other responsibilities would as well—the importance of having a border that is easily crossed and yet appropriately secure, as both governments at the national level would want it to be.

Our economy and our prosperity of course depend on it. Our social and family ties that extend beyond the border do too. It's an interesting fact that each day more than 92,000 cars cross our borders and more than 22,000 trucks carry $650 million in goods a day. Over 66% of all Canada's trade by truck with the US passes through Ontario borders; that's two thirds going through our borders alone. This all amounts to more than $320 billion in trade each year with the US, Ontario's largest trading partner. In addition, a recent Canadian Tourism Research Institute study estimated that border delays cost Ontario more than $5 billion annually. Without new measures to address the western hemisphere travel initiative rules, it has been predicted that Ontario could lose nearly 1.5 million US visitors per year.

1410

Everyone applying for an enhanced driver's licence will be expected to provide documents that confirm their Canadian citizenship. That, of course, emphasizes again that what is important to those at the border is the citizenship of the person who wishes to cross the border. I want to be clear that throughout the development of this program the protection of privacy has been and continues to be a consideration of paramount importance. We have consulted with the Ontario Information and Privacy Commissioner to ensure that the enhanced driver's licence is developed in a manner that protects the privacy and security of personal information. I can assure you that the ministry has no plans to develop a citizenship information database. We are committed to continue working with the commissioner every step of the way. I must say it's a great advantage that we have in this province, having the office of the commissioner, and having the commissioner providing advice to us as legislation is being developed and providing whatever advice the committee deems appropriate during these considerations.

Making sure that all these new cards are issued legitimately is critical to combating fraud and identity theft. One of the ways we can accomplish this is through the use of photo comparison technology. This technology will help ensure that multiple drivers' licences are not issued to the same person under different names. As we know, that's a major challenge for all jurisdictions.

Photo comparison technology has been implemented successfully in many North American jurisdictions, with positive results. Illinois, for example, pioneered this technology nearly 10 years ago and has since discovered more than 5,200 cases of identity fraud. Not only will this increase the integrity of the Ontario card as a pass-

port alternative, but it will also help us stop suspended drivers from improperly obtaining a new driver's licence under a different name.

We know that the Ontario driver's licence is among the most commonly used documents for identification purposes. Ontarians are regularly asked to prove their identity for many day-to-day transactions such as opening a bank account and proving age eligibility for a senior's discount. A photo card for people who do not or cannot drive would improve access to everyday services and would be a convenience for all Ontarians. This has long been advocated by youth, the blind, people with disabilities and seniors' communities. And, like the enhanced driver's licence, our photo card could be enhanced for use as a convenient passport alternative for entering the United States.

Removing barriers to access increases opportunity for everyone. Our government is working closely with the Canadian Border Services Agency and the US Department of Homeland Security throughout its development, and we will continue to do so over the coming months.

I should note at this point in time that I had an opportunity in Washington to meet in a couple of locations with representatives from the United States back when Ontario was pioneering the effort to have an alternative to the passport. This had considerable support, I must say, bipartisan support, in the United States Congress, both in the Senate and the House. I remember one day being in contact with the offices of two different senators who I don't think would agree on anything except the fact that they didn't like this. One was Senator Ted Stevens, of Alaska, and the other was Senator Patrick Leahy, of Vermont. They would not agree on a lot of things, I think I'm safe to say. They were co-sponsoring an initiative within the United States Senate to delay the implementation of the requirements that the US Department of Homeland Security was proposing for the border crossings. We have had many allies on both sides of the border—people of all political parties here in Canada, people of the two main political parties in the United States, people at all levels of government, people from commerce and various agencies that have a particular interest in this issue. I want to commend Representative Louise Slaughter, for instance, who represents New York state. She has a district in the northwestern part of New York state and is one of the really combative persons in the United States House of Representatives on this issue.

In addition to this, the Premier has met with governors in adjacent states and other states that would have visitors frequently visiting Canada and Canadians visiting the United States. So I've been, I must say, very pleased to see the coalition of goodwill that has built up on both sides of the border on this issue.

Ontario is not isolated in this particular effort. Jurisdictions on both sides of the border see a definite need for a passport alternative. To name just a few, Quebec and Manitoba, New York state and Michigan, and I know the state of Washington and British Columbia are pursuing similar programs. Ontarians need safe and secure alternatives and our neighbours, our trading partners and our friends expect us to do our part by taking action to protect the safe and efficient flow of people and goods across our borders by the June 2009 deadline and beyond. I believe the proposed legislation will meet these expectations and the priority objectives of this government.

I want to thank all members of the Legislature because we've had this issue dealt with from time to time in different ways through question period, through debate in the Legislature, through people who have participated in various forums. It has been very helpful to see the degree of support amongst members of all parties. We recognize that there can be quarrels over specifics in legislation of this kind, but it has been encouraging to see that we on this side, just as Americans immediately on border states, have been pleased to move forward.

One of the things that has happened as a result of this initiative on the part of Ontario is that we're seeing the same thing happening in the United States. For us, that is the advantage, of course, because we want Americans to have something other than the passport as an alternative. When June 2009 comes, it's the passport, the Nexus card or an alternative. Other states have been working hard on this, and that's pleasing because not everybody—even though Canadians have a better record—I shouldn't say a better record—have more participation in the passport than Americans, we do believe that Americans with an alternative form of identification are more inclined to visit, particularly the day-trippers, than if they had to go through the process of getting a passport.

I thank all of you today for your interest in this important piece of legislation. I look forward to your input.

The Vice-Chair (Mr. David Orazietti): You're reading my mind. You had two minutes before we began the rotation for questions, but thanks for wrapping that up. We'll start with questions from the opposition. We have about five minutes for each caucus.

Mr. Frank Klees: How much?

The Vice-Chair (Mr. David Orazietti): Five minutes.

Mr. Frank Klees: Five minutes. I thought I had 15.

Mr. Bill Mauro: Fifteen in total.

Mr. Frank Klees: Fifteen in total. We're short-changed again, Minister.

Hon. James J. Bradley: I look forward to your private interventions later.

Mr. Frank Klees: I'm sure.

Thanks for your presentation. You know that we're certainly supportive of the initiative. We expressed, and continue to express, some concerns and I'm hoping that you'll be able to address some of those now with your staff here.

We'll be hearing from the privacy commissioner following your presentation. There were a number of concerns that the privacy commissioners outlined at their meeting earlier this year, in February I believe. You're familiar with those and your staff are familiar with those.

Can you just confirm for us that the concerns that were laid out very clearly and succinctly by the privacy commissioners have been addressed or, if not yet, will be before the implementation of the Ontario project?

Hon. James J. Bradley: Some have been addressed and some are ongoing. I'll get Steve Burnett to comment on this.

Mr. Steve Burnett: Sure. There were a number of—

The Vice-Chair (Mr. David Orazietti): Pardon me. For the purposes of Hansard, please state your name before you proceed.

1420

Mr. Steve Burnett: Steve Burnett. There were a few issues that the commission raised. One was with respect to citizenship and citizenship verification: Would Ontario be establishing a citizenship database and would we be duplicating process? It was properly within the purview of the federal government. We will not be establishing a database of citizens in Ontario. We will be issuing an enhanced driver's licence, which is prima facie evidence of citizenship but not in itself a confirmation of citizenship. So we're not establishing the database.

There was a concern raised with respect to the radio frequency identity technology in the card. That is a requirement of the Department of Homeland Security. It's an imposed standard. If we want to implement the enhanced driver's licence program and have it accepted, that's a condition of that acceptance. We have taken steps to ensure that the card itself can't be read without the user's intervention and part of the implementation includes a protective sleeve, which a number of other jurisdictions are also proposing, which essentially blocks the card and makes it opaque to readers unless it's removed from that thing.

The other piece is potentially around the implementation of the photo-comparison technology, which compares images. There was concern that potentially the application or the scope of this could be broadened beyond this initial implementation. The act itself is very specific with respect to the uses of that technology and actions that we can take as a result of findings of that technology. This is not a totally automated process. Once duplicate images are found, there's staff intervention and adjudication before any action on the part of the registrar.

Mr. Frank Klees: With regard to the RFID, I have a paper here that was submitted through the Consumers Council of Canada that refers to "none of these provinces have gone beyond reiterating the false and misleading claims that since the number on the EDL's chip is random and 'meaningless' it contains no personal information" etc.

You're familiar with this, no doubt. Could you just very briefly comment on that? It's a strong accusation, that we're dealing here with false and misleading information. What assurance can you give us that we are in fact dealing with good information here and that the direction you're heading can be reassuring to our citizens?

Mr. Steve Burnett: The radio frequency ID technology that we're using—generation 2 high-frequency technology—is standards based. There are basically four areas where data can be stored on that chip—96 bytes of information total—and there's no personal information. It doesn't contain the information on the face of the card and it has no identifying information about an individual on the card. The information in the card is a serial number, which is the chip serial number applied at the time of manufacture, and then an ID, which is the key for the receiving organization to access information on the Canada Border Services site. There will be no personal information exposed through the card and the card itself will be protected with a sleeve, unless the individual takes it out.

The technology choice—again, I come back to this—is a technology choice that is driven by the DHS requirement. In terms of the representation that was made, the Department of Homeland Security did publish a notice of proposed rule-making. A number of jurisdictions and a number of technology providers responded to that and based on the input from those sources there was a final determination of the technology.

The Vice-Chair (Mr. David Orazietti): Thank you. That has concluded the five minutes of time for your caucus. Mr. Bisson?

M. Gilles Bisson: Une question—

Hon. James J. Bradley: The time goes quickly when you're having a good time, Frank.

M. Gilles Bisson: Toujours.

Mr. Frank Klees: I was just going to ask you a question.

Hon. James J. Bradley: That's good.

M. Gilles Bisson: Seulement une question avant que je débute : pour quelle raison n'a-t-on pas de traduction ici aujourd'hui?

The Vice-Chair (Mr. David Orazietti): Unfortunately, Mr. Bisson, the room is not equipped with translation. If you want a recess to move to a different room to proceed, we can attempt to do that.

M. Gilles Bisson: Non, on peut continuer aujourd'hui. Je veux seulement faire le point que, la prochaine fois, quand tu me vois venir, je veux avoir de la traduction. Okay?

The Vice-Chair (Mr. David Orazietti): Okay.

Mr. Gilles Bisson: Fair enough? All right, thank you. For my colleagues who didn't understand, at times there are points that we need to ask questions in French because we have presenters who may want to do that. That we don't have translation here I think is a bit unfortunate. So there's been an offer to move to the other room, but for the sake of moving things forward, we will go in English, and if anybody has a problem, please let me know and we'll move the room.

I only have five minutes. Man, I've got five or six questions.

Let me ask you the following, really quickly. Tell me, Minister, in one minute or less, because I know you are good at ragging the puck: You've been around here longer than me, and I've been here for a while. I am in support of this legislation; I want to say upfront that I

think it's not a bad idea. But how is this particular initiative going to end the issue of fraud when it comes to people getting licences illegally? Explain to me exactly how that happens.

Hon. James J. Bradley: It's only one component. That's not the primary purpose of this, but it is one of the components, and that is primarily using the photo comparison technology. One of the problems that we have now is that people can have about four different photos. Some of the fraud that has taken place has involved people having four or five different photos and coming in with these kinds of photos. The new technology allows us to compare these and to identify people who are being fraudulent. We have other initiatives under way within the ministry to deal with that problem, but that is not the primary—that's probably a positive side effect of this particular legislation.

Mr. Gilles Bisson: So we agree that at the end of the day this initiative will not eliminate people getting driver's licences illegally.

Hon. James J. Bradley: It is one of the components—

Mr. Gilles Bisson: Explain to me how it's going to happen, different from today.

Hon. James J. Bradley: Well, in the past, we haven't had this technology available to us, and so we had to do things manually: People had to go through the process of checking, people had to inform, police had to inform, others had to inform.

Mr. Gilles Bisson: You're not answering my question. Tell me how this is going to differ from the current system. We currently have a photo on our driver's licence and now we're moving to this new card. Tell me what's new in the technology that's going to allow us to catch people who are trying to get driver's licences illegally.

Hon. James J. Bradley: Mr. Burnett will assist me in that regard.

Mr. Gilles Bisson: There you go. I was waiting for you. Thank you.

Mr. Steve Burnett: The photo comparison technology sits between the counter and the card production system. Once a photo is taken, it's converted into what's called a template and it's compared against the other images in the driver database. If there's a duplicate found, there's a stop put on the card order and it goes into—

Mr. Gilles Bisson: Can I just ask you one question: Do we not do that now?

Mr. Steve Burnett: No, we don't.

Mr. Gilles Bisson: So that's the difference.

Mr. Steve Burnett: That's the difference. It's the automation of that process and the stop on the order.

Mr. Gilles Bisson: So you have basically technology to compare the photos?

Mr. Steve Burnett: That's correct.

Mr. Gilles Bisson: That answers the first question.

Tell me what the European experience is in regard to people crossing the border from France to Portugal or Spain or Italy or wherever it might be. What's the difference over there in regard to how they deal with their security issues versus North America?

Mr. Steve Burnett: To speak generally to that, they've actually eliminated the borders and the requirements. So there isn't the same attention to border crossing within the EU.

Mr. Gilles Bisson: So I hate to say it, but my friends south of the border are taking this maybe to an extreme. Is this, at the end of the day, maybe not a good thing for our economies in the long shot?

Hon. James J. Bradley: What's good for our economies? Having no border?

Mr. Gilles Bisson: No, I wouldn't argue that for two seconds, not as a New Democrat. My point is that the Europeans—you and I have travelled around the world and seen how they do things in other places. My experience is that when I travel across the border to France or Italy or wherever it might be, there's much less rigour when it comes to security than we have in North America. In Europe there tends to be not any more or any less activity as far as terrorism from one country to the other. So at the end of the day, is this really about making us look as if we're doing something, or really doing something in the right direction?

Hon. James J. Bradley: I would say this will have an effect. Let's face it: Years ago, if you and I crossed the border, getting across the border was pretty simple. They asked one question: "What is your citizenship?" You said verbally what your citizenship was. They asked you where you were going, you said where you were going, and they waved you through.

After 9/11 happened, that of course is not the regimen that you're going to face at the border, and there's considerable concern in North America that our neighbours in particular are a major target. We could be a target as well, but our neighbours to the south of us are a major target. We believe that this will be a piece of technology and a card that will help us to cross the border easily, yet still with security.

1430

The Vice-Chair (Mr. David Orazietti): That concludes the time for the NDP caucus. Mr. Mauro.

Mr. Bill Mauro: First of all, Minister, I want to congratulate you on bringing the legislation forward. I do remember, not that long ago, in the House, when you were in a different portfolio and this issue was first getting broader attention. In your former portfolio as Minister of Tourism, you led a bit of a charge and a battle, I would say, as one of the first people in Canada and certainly in Ontario, when others whom I won't name had thrown up their hands and felt there was very little to do about this. I remember those moments in the Legislature very clearly, and I congratulate you on that.

I wanted to confirm a few things, one being that while there will be a cost attached to the enhanced driver's licence, this in fact is completely voluntary. No one, when they are trying to get a driver's licence, will be required to get the enhanced driver's licence, and the cost

will remain the same under the old system. It will be their choice should they wish to do this. Is that correct?

Hon. James J. Bradley: That is correct. There's always a concern that you're going to impose a mandatory requirement on people. This is strictly voluntary. This is for people who decide that perhaps they don't want to have to carry a passport with them all the time, they don't want to go through getting a Nexus card, so they want another option available.

What's as important to us in Ontario is that adjacent jurisdictions are doing the same thing. Quite frankly, Canadians are more inclined to get a passport than our good neighbours to the south. Our numbers show that fewer Americans have a passport than Canadians, so having this alternative available in states along the border in particular, where there's a lot of visitation here, will be of benefit to us and a convenience to those in the United States.

Already, we have won a couple of concessions. We put it in our Ontario submission—I'm sure lots of other people did as well—that kids 15 and under would only require a birth certificate and that groups of kids 18 and under coming as a hockey team or a band crossing the border would not have the same requirements. So we're seeing some movement that initially was not there in the Department of Homeland Security, and I'm encouraged by that.

Mr. Bill Mauro: On the embedded chip technology, it's been expressed, I think, to some of us that there's some concern around that technology being used by others to steal information that might be contained on the card. It's my understanding that should someone have a scanner or a reader, they would not be able to get any of the information that's on the card, but in fact they'd only be able to get a serial number. You'd actually have to be able to hack into the computer that has the information in it; otherwise, that embedded chip technology poses no risk, in terms of information being stolen, to the general public. I'm just looking for confirmation of that.

Hon. James J. Bradley: That is correct. I'll get Sam Erry of our ministry to elaborate.

Mr. Sam Erry: You're quite correct in terms of what data will or will not be accessible. It's basically a series of numbers, and if you can do something with that, then great, but the likelihood of that happening is extremely low. As Steve Burnett indicated, we're also providing a protective sleeve, a Faraday sleeve, for the card so there's no opportunity for anyone to take the information.

Mr. Bill Mauro: The last question is on the photo technology piece that's being implemented. Through this enhanced driver's licence, there's the potential for fewer people to be able to get duplicate driver's licences in the province of Ontario, should people voluntarily avail themselves of that particular licence. Is that correct?

Hon. James J. Bradley: Yes, that would be correct. It's one of the components of trying to reduce fraud. It's not the only component, but it's a significant component to have the photo comparison technology available to us.

The Vice-Chair (Mr. David Orazietti): Thank you, Minister and staff, for your presentation today. That concludes the time.

Hon. James J. Bradley: It's a pleasure to be before the committee, and I await your deliberations.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The Vice-Chair (Mr. David Orazietti): I'd like to call on the Office of the Information and Privacy Commissioner of Ontario. Dr. Ann Cavoukian, thank you for being here today, and welcome to the committee. If anyone else will be speaking again, for the purposes of Hansard, introduce yourself and proceed. You have about an hour for your presentation, so if you'd like to get started, go ahead. Just one other reminder: Any time that is not used by your presentation will be distributed among the members for questions.

Dr. Ann Cavoukian: I'd like to begin by thanking the Chair, the Vice-Chair and the members of the Standing Committee on General Government for the opportunity to make a presentation today during your 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 the most important duties that I have. I also believe that it is vitally important to be practical in the protection of privacy and ensure that the right information reaches the public at all times. 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—and I totally agree that this is a completely voluntary venture.

The primary purpose behind this proposed bill is to enable the government to issue an enhanced driver's license, as you've heard—I'm going to refer to it as an EDL—which is intended to serve as an alternative to a passport solely for the purposes of entering into the United States. In addition, Bill 85 provides the government with the authority to issue new photo cards for those who do not or cannot hold a driver's license, such as people who may have a visual impairment. Such photo cards are available in virtually all other provinces in Canada. 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'm going to refer to as WHTI, which is the common use of the term—has grown out of security concerns following the events of 9/11. As an individual citizen, I certainly understand people's fears relating to terrorism; however, as commissioner, I also

fear the potential loss of our freedoms, especially our privacy, which forms the basis of all other freedoms. In the days following 9/11, many people, especially those in the United States—many of my colleagues in the US—were reluctant to speak out on behalf of privacy for fear of being viewed as unpatriotic. I remember those days vividly.

I had a call, in response to a call from the CBC a day or two after 9/11—they called me seeking my position on the events that had transpired. It was a very difficult position to be in, and of course I had to issue a position, which I did. I issued a position paper, which was posted jointly to our website—CBC and ours. The heading was Public Safety is Paramount—But Balanced Against Privacy. The position I took was that of course we had to protect public safety, but—and it's 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—and it had to be real. I argued that our search for safety and security could not come at the expense of privacy, that this would be a fundamental error. Forfeiting our privacy in the pursuit of security is simply too high a price to pay.

Having said that, I want to make it 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 say, for the record, that I am not opposing the government's commitment to introduce an alternative to a border crossing document such as a Canadian passport.

1440

If we have time during question-and-answer period, I'll remind you how this came about and it's actually the lesser of two evils. I just want to make sure that privacy is built into the program. Many people say, "Well, you could just get a passport." I share those views in part because I have a passport, but I regularly travel and I need a passport to get into other countries. Many Canadians do not have a passport and, for whatever reasons, the public, especially in cities across the border, want it. This is their view and it's not my place to tell them that they can't have this. My place is to comment on the privacy implications.

Let me tell you, first, that over the past year my office has developed a very good working relationship with the Ministry of Transportation. Minister Bradley and I have talked a number of times, our staff have talked, and as well with 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 that is acceptable to the US government.

My office has been, I think, quite 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 enhanced driver's licence. We heard arguments from members of both sides of the debate, including the University of Toronto's identity, privacy and security initiative, an excellent program at the University of Toronto, as well as from representatives of both provincial and federal governments, and consumer and citizen interest groups such as the Consumers 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'd like to give you now a brief overview of my privacy concerns relating to Bill 85.

After careful, very extensive study, we noticed that Bill 85 was missing several privacy principles commonly included under internationally recognized principles called fair information practices. While each of these principles is detailed in my submission, which is extensive, let me just discuss one of them briefly here that speaks to the question of accountability. Openness and transparency, as you know, are key to government accountability, especially when the government serves as the custodian of a significant amount of personal information on its citizens.

My concerns here relate to Bill 85 leaving crucial matters affecting the privacy and security of Ontarians either to the discretion of government officials or to be later prescribed by way of regulation without any requirement for public notice or comment. These matters are not defined in Bill 85, and Bill 85 does not list the specific personal information to be collected, used or disclosed by the government.

For example, the information to be contained on the photo card is not detailed. The security and other features that may allow the photo card to be used for travel purposes are not detailed. The information that the Ontario government will collect from municipalities and other provincial, territorial and federal government departments and agencies is, in my view, 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 are not present. The requirements for being issued a photo card are missing. These are the details that can be added to enhance the quality of the bill.

Mr. Gilles Bisson: Excuse me. I wonder if we can get the outside a bit more quiet.

Dr. Ann Cavoukian: I could try to speak up a little.

Mr. Gilles Bisson: No, it's not your fault. There are people outside and I'm having a hard time trying to listen here.

The Vice-Chair (Mr. David Orazietti): Mr. Bisson, we'll take care of that.

Mr. Gilles Bisson: Can we put her time back on, please?

The Vice-Chair (Mr. David Orazietti): Go ahead and continue with your presentation. We'll have someone take care of that.

Dr. Ann Cavoukian: I'll speak a little more loudly.

Mr. Gilles Bisson: No, it's not your fault; it really isn't.

Dr. Ann Cavoukian: Thank you.

Under these circumstances, in order for transparency—before I begin, since there was a small break, forgive me; I forgot to introduce my colleagues. I sincerely apologize for that. I go by the script and it wasn't in the script—my omission. I'm joined by my assistant commissioner of privacy, Ken Anderson, and Michelle Chibba, my director of policy. They have both worked extensively on this file with me and I'm very, very grateful for their efforts. I apologize for the omission.

Let me resume. Under these circumstances, in order for transparency and accountability to be achieved, the regulation-making powers provided 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 actually set out in legislation. Other instances include the Personal Health Information Protection Act, which was introduced in 2004 very successfully; 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 goal based on the wording contained in Ontario's Personal Health Information Protection Act, which I referred to earlier.

With regard 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 face-recognition software application that will convert a photograph, as has appeared on a driver's licence for many years, into a biometric template to allow automatic comparisons behind the scenes within the ministry's database of drivers' 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 such as a photograph, will only be used internally and restricted solely for the purpose of verifying the identity of card holders, full stop. Placing strict controls on its use is absolutely crucial.

In the remaining time, I'm going to devote my comments to two important areas: verification of citizenship information and, of course, the radio frequency identification technology, or RFIDs.

First, let me briefly discuss the issue of citizenship verification. Earlier this year I was so exercised by this that I actually went so far as to issue 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 have been asked to verify the citizenship of applicants for the purpose of the EDL program. Applicants will have to provide proof of Canadian citizenship to the Ministry of Transportation and complete a questionnaire with very intrusive questions. I'm not going to detail the questions now; I have a few examples if we have time in question period. Finally, they have to undergo an in-person interview.

This is baffling to me. 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. Please, this isn't something new. We have several precedents, other examples, where secure information-sharing between our federal and provincial governments has taken place. If the federal government has some information in its possession and a province needs it, surely we can, securely, have that information conveyed to that province without having to have the province go through the entire exercise from scratch.

One example is Ontario's Gains program, which receives tax status information on individuals from the federal Canada Revenue Agency, which possesses that information. This has been in place for years; it works beautifully and securely, no problem.

Mr. Gilles Bisson: What's it called?

Dr. Ann Cavoukian: The Gains program, and we get that from the Canada Revenue Agency.

I initiated a dialogue with the Honourable Stockwell Day, Minister of Public Safety, some time ago—he's responsible for national coordination of the EDL program—to request that the Department of Citizenship and Immigration 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 what's called data minimization should and must always prevail, meaning quite simply that if you don't need to collect and create new personally identifiable information, don't do it. Minimize your data collection, because that is the best way to protect information instead of recreating it, retaining it and then having to securely protect it.

1450

Requiring provinces to build their own pockets of citizenship information from scratch—in effect reinventing the wheel—when the federal government already has that information needlessly adds to our privacy and security concerns, not to mention the unnecessary financial and human resources 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, especially at this time of great economic crisis, 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, for one example, and add to the potential unintended consequences of error and inaccuracy that invariably would arise in the process of

recreating already existing information. Unless you think this is a simple yes/no answer to citizenship, and I assure you it is not, this database—or call it what you will. I know some people say we're not going to recreate a database—a file. Call it whatever you want. This 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 then has to be forwarded to the federal government in any event, resulting in further duplication cost and privacy risk. This is no simple matter, so please let's not complicate it any further.

Let me be clear: I know this is a federal issue; it's not the doing of our Premier or our Minister of Transportation. I give you that. But regardless of the fact that it was a problem created by the federal government, we have to resolve it; it has to be resolved now. The federal government already has this information. It has the ability to easily verify the citizenship of natural Canadians and to securely provide that information to a province such as Ontario upon request. This is clearly a more privacy-protective and cost-effective solution, a real win-win solution: more privacy and security, lower cost. Surely there's no contest here.

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, as I'll refer to them. For any of you who may not be familiar with RFID technology, I'll give a very brief introduction to the topic, and I do mean brief. RFID, as you know, is a generic term for a variety of technologies that use radio waves for the purpose of automatic identification, consisting of two integral parts: a tag and a reader. For the tag, you can think of a bar code on steroids. It's a bar code because it's an identifier, and it's on steroids because it beams out where it is. There are two main types of RFID tags, active or passive, which differ depending on whether they have their own power system. A passive tag has no power source and no on-tag transmitter, and that's what's being contemplated now in the EDL program. Finally, you need to know that RFID tags are activated by readers, wherever they may be, which in turn are connected to a host computer. In a passive system, the RFID transmits a signal via the air waves that wakes up the tag by powering up its chip, which in turn enables it to transmit data. So in the kind we're contemplating on the EDL, the chip contained in the driver's licence is asleep until it's, as they say, pinged. So a reader pings it and says, "Is there anybody out there?" If you have an active, meaning a functioning, tag, it will receive the message and be woken up and say, "Yes, I'm here," and it will release, via the radio frequencies, via the airwaves its identification number. We'll talk about that in a moment.

I should just tell you for your information that I've spent a number of years working in this field trying to secure privacy within RFID technology. My office has produced three papers and a set of practical guidelines on the subject going back five, six, seven years. I'm not opposed to the use of RFID tags across the board, as many privacy advocates are. I'm a pragmatist and proud to call myself a pragmatist. It's got to be practical; it has to be real. I believe that RFIDs can have many benefits, but like all information technologies, they need to have privacy protections baked into them early in the design of the systems involved. I call this "privacy by design." This is a term that I first developed in the early 1990s, which ensures that privacy does not become an afterthought, because it has to be built right into the system. Tagging things in areas such as the supply chain management process or taking an inventory of assets poses no risk to privacy. That's why I haven't objected to the use of RFIDs when there are no privacy concerns, when there are no individuals involved in supply chain or inventory of assets. However, tagging things linked to people can raise serious concerns about the relative permanence of the tag, the nature and amount of data to be collected and the strength of the data's linkage to personally identifiable individuals. That's what's key: data 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 identified, that's when privacy concerns arise.

How does this relate to Bill 85 and EDL? Currently, US customs and border protection, CBP, uses RFID technologies on its trusted or registered traveller 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 travellers crossing the border." The Department of Homeland Security requires that any approved border travel document carry an RFID tag, and that's what brings us to all of this, because you might say, "Why do we need this?" And that's a question you can pose to others. That is not the issue I'm going to address. I want to tell you that at the program we had in the summer—the public forum—we had a number of people who spoke out in favour of the EDL. I'm going to quote from one of them.

Arlene White was the 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. She spoke at the summer forum, as I mentioned, about the vital importance to border communities and their very strong support for this program. I was surprised, actually, and after her talk, during question period, I asked her a question: "Are you telling me that having the RFID capacity to cross the border when you're in the car is really going to enhance speed that fast and it's really going to make a difference?" She said, "Absolutely." She emphasized the desire of these individuals in the border towns to ensure the continued smooth flow of traffic at their borders which, in her view, would simply not be possible without this RFID technology. I'm only reporting that to you; I can't substantiate that or not. But that is not only her view but the view of her group, so I wanted to pass that on.

Let me give you some sense of what all this means with respect to privacy and security. A fundamental

characteristic of all RFID technologies is, as I said, that they're wireless. This means that any data contained on the chip—in this case the unique index number, which you heard about earlier, which is stored on the embedded RFID chip—is transmitted through an RFI reader that pings it to a database of information. This number serves as a pointer to the individual's personal information contained in the database—

Mr. Gilles Bisson: What's the number?

Dr. Ann Cavoukian: I'm calling it the unique index number, and it is what is pinged and transmitted and collected. Then, that is used as a pointer in the database to access information needed for border crossing purposes. There are well-known privacy and security vulnerabilities associated with RFID technology. These are commonplace. They apply to any RFID-enabled identification card and information system. I'm going to mention just three of them.

One is skimming. This occurs when an individual with an unauthorized RFID reader gathers information from the chip on the card without the cardholder's knowledge. Remember, the RFID is emitting radio frequencies that can be picked up by any reader in the area, authorized or unauthorized. It doesn't discern which reader it should transmit the radio waves to. If you have an unauthorized reader and you're in the area, you can pick up the information that is accessible. That's skimming.

Number two is eavesdropping. Eavesdropping occurs when an unauthorized individual intercepts data using an unauthorized RFID reader. So not only can you access the information, but you eavesdrop. You pick up the information.

Third is cloning, which occurs when the unique information contained on the original RFID chip is read or intercepted and its data are then duplicated; a copy of it is made.

1500

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 goodbye to privacy.

In response to some of these concerns, you have been told that the RFID Gen 2 standard, which is the standard being used for this EDL—which again, I will repeat, is being required by US Homeland Security, so it's something we must use. This standard does not include any personally identifiable information, you've been told. It only has a unique number, this index number, which links the cardholder to his or her record in a database. So people say, "There are no privacy concerns, right? It's just a unique number." Wrong. Think of a social insurance number. A social insurance number is just a number. It's a string of digital identifiers. Think of a passport number; think of a driver's licence number. In and of themselves, they're just a string of numbers of no use to anyone who finds them. But once you link it to personally identifiable information, each of these numbers can be subject to great abuse by unauthorized parties or they can be 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 not inconsequential. It's not just a meaningless number. It points to real, personally identifiable information that may then be subject to abuse. When you think of the social insurance number, it's often referred to as the key that will unlock many doors, because the social insurance number is unique to you. It is a unique personal identifier that of course, as a string of numbers, 441-451—I guess I shouldn't give you the rest of my social insurance number. I know it by heart. But the point is, it is linked to me, and once it's linked to me, a lot of personal information is enabled. In the United States, the social security number: the same thing; the same fears associated with it. That's the golden key.

So I just want to make this point: that just because it's a number and it doesn't have a name linked to it does not mean it cannot be linked to personally identifiable information. That's what we emphasized in our papers on radio frequency identifiers. The capacity for data linkage is what creates the privacy risk. 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 that this sounds like a really wildly futuristic scenario, but I assure you it is not that far off. In the here and now, right 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 now entered into the scene en masse. This is an area we have to be concerned about and watch out for.

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 were encased in this sleeve. Some call it the Dorito chips method of protection, because a Dorito chips bag has aluminum foil, and that essentially does the trick. But in my view, this is not a sufficient answer. The cardholder must take on the added inconvenience. But also you have to remember to put your card into the device, and I don't think it's going to happen.

Could someone give me a credit card, if you would? Thank you. Here's a driver's licence. Here's the Faraday cage. First of all, I have to get it in the cage. Maybe more of you are better than I am—here, I got it in, but it takes some doing. Then I have to put this in my wallet. I can tell you, this will not fit into the little tiny thing—the slides that are available in your wallet now? It won't fit with this. So people are going to make a choice. They're either going to say, "To heck with this; I want to keep it

in my wallet," which is the whole point of the exercise, or they're going to try to do this and they're going to get fed up with it and they're going to abandon it. In my estimation, this is not an acceptable solution.

I don't want you to take my word for it. If you go into the literature at all in this area, everyone—the techies—all laugh at this as the solution to the problem. This is not an acceptable solution in the literature among both technologists and privacy advocates.

In my view, again, it's not the answer. The cardholder has the added inconvenience and has to remember to put the device in the Faraday cage.

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 or the unique index number by unauthorized RFID readers until the cardholder remembered to actually place it successfully in the card sleeve. This solution is only protective when the individual remembers and succeeds in placing the card in the sleeve; otherwise, the reading of the cards are free and clear.

I'm going to read you a quote in a moment, but I have to tell you, there are groups of people—what are they called? Wardrivers?

Mr. Gilles Bisson: Wardrivers?

Dr. Ann Cavoukian: Wardrivers. I know; it's a weird term. They're techies who do this for fun. I don't want to call them "hackers" because many of them are good hackers, but they drive around, and it's what they do for fun. Instead of playing a video game or something, they drive around and they try to pick up signals from RFIDs. You would not believe how successful they are. They drive around and they have their unauthorized readers on and they try to intercept signals. I don't do this, but I know of people who have done this, and they tell me how successful it is to do it.

Even leading researchers, such as Sophia Cope, staff attorney and fellow at the Center for Democracy and Technology, agree that this method of the Faraday cage is hardly sufficient. In her testimony before a Senate committee in the United States 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 will "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 drivers' licences 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."

She's going farther than me. She's saying that even if you use a Faraday cage, at some point you've got to take it out of the cage in order to actually have it be successfully used for whatever purpose it was intended. At that point in time, it is subject to all the risks we were talking about, in terms of skimming, eavesdropping and interception.

In Ontario, people often use their drivers' licence, as you know—

Mr. Gilles Bisson: So it transmits once it's out?

Dr. Ann Cavoukian: When it's out of the Faraday cage, it is always on. So while it has to be pinged by a reader to get the information—

The Vice-Chair (Mr. David Orazietti): If we can hold the questions until the presentation's over; if we can just hold the questions until—

Mr. Gilles Bisson: We're not going to get any questions. That's why I'm doing it right now.

Dr. Ann Cavoukian: Okay. In Ontario, as you know, people often use their driver's licence when asked for government-issued photo ID. We have all been in instances where you use your driver's licence for ID: to vote, open up a bank account or apply for a credit card; multiple purposes. So the driver's licence is used for many purposes other than for driving, and I'm suggesting that it's going to be used for many purposes other than just crossing the border. That's why we need to make it as protective as possible.

As the RFID standard chosen for this project will respond to any reader query, any pinging, 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 purposes. A better solution than the proposed sleeve is needed.

The way that I always proceed is to go off and look for those solutions, because I always figure that if you've got a problem, you've got to find the solutions and offer them to people. I think we found a solution. 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 card, which can then be incorporated, as I said, directly on the card. So wouldn't it be cool if you could turn it off—just on/off? Wouldn't that be a wonderful thing?

1510

I'm not proposing this based on yet-to-be-developed technology. My team has been very busy scouring the corners of the globe to find some solutions, and we have found some. Several groups are developing this on/off switch. I'll name three.

At MIT, the media lab has already patented and prototyped an on/off switch for an RFID tag that can be incorporated directly into a card, allowing the cardholder to determine when and where their information will be transmitted.

Even better, though, another company based in the UK—this one is really good—called Peratech, has advanced this on/off switch even further. They've developed it using something called quantum tunnelling composite technology. Don't ask me to explain that to you. But I know, because my tech people have looked into it, that it is advanced technology and the founder and CTO of Peratech, David Lussey, advised me that, and I quote—we spoke directly to him—"Peratech's technology is readily available under licence for the appli-

cation of acting as an on/off switch on an RFID driver's licence. 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're talking about." So this, to me, is indeed very promising technology.

But there is a third company in the United States, called Root Labs, which is working on a similar on/off switch that would be placed on transponders to be used by San Francisco Bay highway toll users.

I give you these three examples because people say, "Well, there are no alternatives." There are alternatives, and we make a point of finding those alternatives and offering them as solutions.

I brought together representatives from our government and the vendor that has been selected to produce EDLs in Ontario, hoping to advance this very promising technology that I believe should be seriously considered for EDLs in Ontario. I thought it was necessary to bring everyone together with the goal of advancing the feasibility and the development of this very promising technology. In fact, a senior executive from the government's own selected vendor told me the following: "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," otherwise known as G&D, the vendor of choice in Ontario, "is working diligently on the development of our own technologies and assessment of third party technologies to enhance RFID functionality, security and privacy."

This is wonderful to me. These present viable options that can be pursued, and I ask you to stay tuned because, rest assured, we will be exploring these with the Ministry of Transportation and with the selected vendor.

Let me shift gears now and give you just a little bit of perspective by way of background on privacy and technology, and I'll be ending it shortly after that.

Since the early 1990s, I've been advancing the idea that technology has the ability not only to provide for good security but also to provide for good privacy. In 1995, I put forward the view that technology can liberate us from what I called the zero-sum trap of having to sacrifice privacy in order to have security. When you think of a zero-sum game, it requires an advancement of one interest at the expense of the other, and when you have security versus privacy, invariably privacy loses. So that's why I have developed this, what I call a positive-sum paradigm. Forget zero sum. I want you to give me both security and privacy, together in the same device.

We cannot view privacy and security as polar opposites. In this view, in this new positive-sum, win-win scenario, privacy and security can both coexist because technology is enlisted to protect privacy and safeguard personal information through privacy-enhancing technologies, or PETs. When applied to technologies and surveillance, PETs can serve to transform these technologies into ones that are protective of privacy. Hence, I've developed a new term—you might call it PETs-plus—and it's called transformative technologies. Why have I done this? I've done this because, whenever I enter into an arena talking privacy alone, privacy-enhancing technologies, "I want you to address privacy"—if I'm talking to a tech company or a security company or a business, invariably they lose some interest, because they think my focus is exclusively on privacy. That's not true. I want you to give me privacy as well as whatever else that technology is intended to do. So you want to do video surveillance cameras? You do that and you give me privacy, and we'll tell you how to do it. The University of Toronto has developed a very ingenious way of doing that. I digress, but PETs-plus is transformative technologies, and the reason is, if you talk about transformative technologies, you get the interest of the security companies and the biometric companies and the technologists. People listen, because I'm not asking you to abandon security for privacy; I'm asking you to give me both, and I'm insisting on both. They accept that messaging better.

I digress. Transformative technologies, using this positive sum paradigm, which just means security and privacy, embeds a privacy-enhancing technology to what would otherwise be considered a privacy-invasive technology: video surveillance cameras. You apply privacy-enhancing technology, you give me both privacy and security and you transform what would normally be considered a privacy-invasive technology—surveillance cameras—into a non-privacy-invasive technology, because when you apply what I'm talking about, the encryption program, to this technology, all you get—if you had a camera on me, you would just get the background footage; you would not get personally identifiable information relating to me unless you had the encryption keys. So that's why it transforms an otherwise privacy-invasive technology into a privacy-enabling one. I call this, as I've said before, privacy by design, and it is literally my mantra, the mantra of my office. 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 without losing the functionality of that technology. That is key. 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.

So in the spirit of all of this, I'm recommending the following with respect to the use of RFID technology in the EDL. First, I'm recommending that any use of radio frequency identification technology comply with the RFID guidelines set out by my office, and I've brought a few copies with me. We created these two or three years ago, and we've updated them recently. Second and most important, I recommend that the ministry work with a 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, which means any time other than

crossing the border. I want to tell you that I have spoken directly to the vendor and to ParaTech and to these other companies, so I'm not leaving it up to chance. It is definitely within the range of possibility to do this. One of the biggest obstacles is the standard that has been offered by the US, the Department of Homeland Security, and we've opened up channels there. As you know, there is an election that will take place in the United States, there's the possibility of a change of administration. Who knows. Stay tuned. But we have recently spoken. Just two days ago I spoke to members of the Department of Homeland Security with a view to opening up the dialogue and changing the standard, which would enable this stronger protection to take place. So stay tuned.

Let me conclude by sharing a motto that my office developed some time ago and that we follow religiously. I call it the three Cs. Perhaps I should call it the four Cs, because it's a bit corny. But here are the three Cs: consultation, collaboration and co-operation. This philosophy represents the ethos of my office, and I think it's an attitude that we all share in my office. I know I carry it into our work regarding the EDL program. We want to make this work. We're not trying to throw up roadblocks, but we want to make it work in the most privacy-protective manner possible. So I'm not opposed to the EDL program. I have these concerns regarding privacy. They're outlined in our lengthy submission, and I feel they have to be addressed based on the mandate that the Legislature of Ontario has given me. I look forward to serving that mandate in the spirit of the three Cs.

Thank you once again for providing me with the opportunity to appear before you today and for considering my office's comments on Bill 85. I'm confident that with our continued collaborative efforts, we will be able to appropriately address any outstanding privacy matters and best serve the interests of the people of Ontario. In fact—and this is what I would like to do—we could develop the most privacy-protected EDL available anywhere in the world. We can do this here in Ontario, and it would be another first for Ontario because we shine in the area of privacy and technology. Hopefully, we can do that together. Thank you very much.

1520

The Vice-Chair (Mr. David Orazietti): Thank you very much for your presentation. Mr. Klees, if you'd like, each caucus will have five minutes for questions.

Mr. Frank Klees: Thank you very much. Commissioner, I want to thank you and your team. I'm into my 14th year of hearings in this place, and without question your presentation today was one of the most enjoyable and informative presentations I've ever heard.

Dr. Ann Cavoukian: Thank you so much. You're very kind.

Mr. Frank Klees: I want to thank you for the stock tips as well

Interjection: Yes, we wrote them down.

Mr. Gilles Bisson: There's no such thing as a good stock tip.

Dr. Ann Cavoukian: I didn't know I gave stock tips.

Mr. Frank Klees: I don't know. Based on what I heard, I think we have some real possibilities. We heard from the minister earlier, and he made the point of saying that he's been consulting with you.

Dr. Ann Cavoukian: Yes, he has.

Mr. Frank Klees: I agree with him that I think we're very fortunate to have someone of your stature as an officer of the Legislature. I'm hopeful that the minister and his staff will in fact do what they said they'd do, and that is to take your advice seriously. We've seen this government in the past hear your advice and not take it, to its detriment. I'm going to be hopeful that the very solid presentation that you made and that the recommendations you've brought forward will in fact be taken back by ministry staff and that they will work with you. We will do what we can to hold the government accountable on these very important privacy issues. I'm convinced that the minister is sincere when he states his commitment to meeting the privacy issues and challenges. I've done a lot of reading on this as well, and I've put it to the minister that there are a lot of questions about the technology, so what's encouraging to me is the research that you and your office have done to bring what I believe to be real solutions to what all members of this committee, I'm sure, and all members of the Legislature are concerned about.

I have another question for you, though. I was surprised to hear you say that the application process for this card is as complex as you describe it. I've just gone through the Nexus application process, and from the sounds of it, it was more straightforward than what you're describing here.

Dr. Ann Cavoukian: You're right.

Mr. Frank Klees: I can now bypass, as you well know, all of the lines of security, and I'm on my way because of the pre-approval that I've gone through. But what you're talking about is actually more complex than what I had to go through, but those people don't have the benefit of a pre-approved card. Can you just comment on that? How do we cut through that?

Dr. Ann Cavoukian: I will. Thank you very much, Mr. Klees, for your kind remarks.

I'm going to ask Ken Anderson and Michelle Chibba to respond, because I couldn't believe it either. You would not believe the questions that these people have to answer. I couldn't believe it, so I'm going to ask directly. Michelle has them here. We're going to respond to this.

Mr. Ken Anderson: Michelle's put a lot of work in this area. She might start off, but I can tell you one thing—

The Vice-Chair (Mr. David Orazietti): Please state your name for the purposes of Hansard. Thank you.

Mr. Ken Anderson: My name is Ken Anderson. I'm the assistant commissioner for privacy, and my colleague Michelle Chibba will comment after me.

We have, in working on this file, also met not just with ministries in Ontario but also with federal counterparts that are a part of the entire system. We too have

been surprised at the nature and extent of the application process, and we had asked questions saying that we don't have to do this for a regular passport, so it's rather surprising to do this. The sense we had was that you don't have to do that now, but maybe at some point that would change. Certainly Michelle could tell you some of the questions in the process.

Ms. Michelle Chibba: I'm Michelle Chibba, director of policy at the IPC. What we've taken, in terms of public information that we're allowed to share, is the model that the BC government is currently using. Our understanding is that it's the same set of questions that have been provided by the federal government that all provinces who implement an enhanced driver's licence—that any applicant will have to go through these questions.

The questions are—and I'd like to ask these questions so that you can also think about what the answers are:

—Were you born in Canada?

—At the time of your birth, was one of your parents a foreign diplomat, consular office or representative or employee of a foreign government recognized by the Canadian government?

—Have you ever renounced or given up your Canadian citizenship? If yes, please provide the date you renounced it.

—Did you ever take or sign an oath renouncing your citizenship before February 15, 1977? If yes, please complete question (e). If no, skip (e) and go to question (f).

I will ask you question (e): If yes to question (d), were you under 21 years of age at that time?

—Did you become a citizen of another country before February 15, 1977? If yes, please complete question (g). If no, skip (g) and go to question (h).

—Question (g) is: If yes to question (f), were you under 21 years of age at that time?

—Did one of your parents ever renounce or give up their Canadian citizenship before February 15, 1977? If yes, please complete question (i). If no, skip question (i) and go to question (j).

—If yes to question (h), were you under 21 years of age at that time?

—Did one of your parents—

The Vice-Chair (Mr. David Orazietti): I'm sorry, we're a minute or so over the time. I thank you, Mr. Klees, for your time—

Mr. Gilles Bisson: Go ahead. She can use some of my time to respond. Please.

The Vice-Chair (Mr. David Orazietti): Okay.

Mr. Gilles Bisson: Go ahead. You were going to respond?

Ms. Michelle Chibba: No, I was just going to say the last question: Did one of your parents become a citizen of another country before February 15, 1977?

Mr. Gilles Bisson: So what good does this do us?

Dr. Ann Cavoukian: I have no idea.

Ms. Michelle Chibba: Sorry, we can't—

Mr. Gilles Bisson: So this is the questionnaire that would be asked in order to gather all this information?

Dr. Ann Cavoukian: Yes, plus a live interview with someone. Really, for any of you who have gone through the passport process—now it's really easy to get your passports renewed. Once you have it done once, you no longer need a guarantor; you can do it online. It's a piece of cake. This is much more cumbersome to me and it's unnecessary. We know who the citizens are, we know—anyway, I'm not going to belabour the point, but that's what this is about.

Mr. Gilles Bisson: Let me ask you a very simple question. In its current state, would you support this legislation if you were me?

Dr. Ann Cavoukian: That's a trick question.

Mr. Gilles Bisson: It's not a trick question. We both support—

Interjection.

Mr. Gilles Bisson: No, do it on your own time.

Everybody in this House agrees that this is not a bad idea. My concern, and the reason that I asked for you to be before this committee, is that I have some security concerns. I don't pretend to understand it in detail, and that's why you're here. So my first question is, in its current form, would you support this legislation if you were me?

Dr. Ann Cavoukian: I would like to see the legislation strengthened. In our submission, we have very detailed language and procedures that can tighten it, wouldn't you say so, Ken?

Mr. Ken Anderson: Yes.

Dr. Ann Cavoukian: And I'm confident that Ministry of Transportation staff will work with us, as they have been working with us very co-operatively, and I expect them to be responsive to our recommendations in our submission.

Mr. Gilles Bisson: You have 20 recommendations that you've given us. This may be a bit of an unfair question: Are these all must-dos, or are some of them more must-dos than others?

Mr. Ken Anderson: There's always a sense of gradation, I suppose, when one reads a list. We think that they're all important. We have the sense that they're all doable and we're working very hard to ensure with the ministry that it's completed on behalf of Ontarians.

Mr. Gilles Bisson: My next question is that—and we only get five minutes; this is the unfortunate part. You're saying that we need to have a public consultation around the regs, because we all understand that this is all going to be left up to regulation. If there isn't a spelled-out process in order to have public consultation on the regs, should I support this?

Dr. Ann Cavoukian: I can't answer that for you. That is a matter for your conscience.

Mr. Gilles Bisson: I hear you. You gave me the answer I was looking for.

How much time have I got?

The Vice-Chair (Mr. David Orazietti): About a minute or so.

1530

Mr. Gilles Bisson: The unfortunate part is—and I throw a pox on all our houses, all parties that have been

in government—we've rushed this type of legislation through. Listen, it's my fault, it's your fault, it's all our faults. We try to rush this type of legislation through without giving it the type of consideration that we need in order to get it right. What I fear is—we're trying to do the right thing here—if we don't take the time to figure out what technologies to use and how to do it to protect privacy, we may be going down quite completely the wrong road. So I just want to put on the record that I find this somewhat rushed. Actually, I would propose a motion at this point that we bring you back before this committee next week for some more time, because we need to ask some pretty specific questions.

I would move a motion that we bring you back before this committee next week so that we can ask you some questions, so that we have a better sense of what it is that we need to do as legislators.

Dr. Ann Cavoukian: I should just say that I'm confident the ministry will be responsive to our recommendations and I look forward to working with them. I think we can really improve the legislation.

The Vice-Chair (Mr. David Orazietti): Okay, thank you very much. At this point, the subcommittee has made a recommendation. If that changes before next week, then I think that's a matter for the subcommittee to discuss. At this point, we're going to move on to the Liberal caucus for—

Mr. Gilles Bisson: Chair, point of order: To the clerk, it's well within my right to move a motion at this time, so I'm moving a motion that we bring the privacy commissioner before us next week.

The Vice-Chair (Mr. David Orazietti): Any debate on the motion?

Mr. Gilles Bisson: No debate? I take it we're all in favour of—

The Vice-Chair (Mr. David Orazietti): Seeing none—

Mr. Gilles Bisson: Recorded vote.

The Vice-Chair (Mr. David Orazietti): Mr. Brown?

Mr. Michael A. Brown: I just wanted to point out that from the government's point of view, we take direction around here on the basis of consensus. The subcommittee has met. The subcommittee made recommendations. If you wish to take this up with the subcommittee, I think that would be totally a real possibility. If not, however, we would be pleased to vote.

Mr. Gilles Bisson: This issue has been raised by the subcommittee and it's something that we talked about. My specific request during the subcommittee time was that we be given enough time at committee to make sure we hear what we need to hear to do our jobs here as legislators and if we needed more time that we would use it. That's why in the subcommittee report we're talking about extra days if needed. I think what we are hearing here today is that the commissioner is supporting the general intent of the legislation and all members of this Legislature are; nobody is opposed to the idea, we just need to get it right. I would ask that we have a vote on having her come back before this committee so that we can ask some questions in order to make sure that we understand what some of these concerns are.

Mr. Michael A. Brown: In order to be very helpful, I would suggest that we ask the member if he would like to wait till after the proceedings are finished today—

Mr. Gilles Bisson: No, I want the vote now.

Mr. Michael A. Brown: —which shows to me that we're done by about 5 o'clock or 5:30. There's plenty of time to discuss it then—

Mr. Gilles Bisson: No, I would ask for the vote.

Mr. Michael A. Brown: —and we can then vote. I think that's a reasonable and sensible way to order the committee's business.

Mr. Gilles Bisson: Again, I think—

The Vice-Chair (Mr. David Orazietti): Just one second, Mr. Bisson. There's a motion on the floor at this point, so any further debate on that motion? Ms. Mitchell.

Mrs. Carol Mitchell: Yes. I just wanted to speak specifically to this motion as a member of the subcommittee. We specifically allocated an hour of time for the privacy commissioner—

Mr. Gilles Bisson: Thirty minutes

Mrs. Carol Mitchell: —on the recommendation of the subcommittee members. We read into the record the recommendations at the very beginning and this is the hour that we had agreed upon prior to the hearings. So I just wanted to make the committee informed of that subcommittee decision.

The Vice-Chair (Mr. David Orazietti): Further debate?

Mr. Gilles Bisson: I was on the subcommittee as well and it was pretty clear that my recommendations and my concerns were that we had to do this right, that the New Democratic Party supports the initiative the government is putting forward, but we need to make sure we get this legislation right. I asked, at the time of the subcommittee, if more time was needed that we take that time. I said we would not try to delay this legislation in any way, we just want to make sure we get it right. I think there are some very important points that have been brought before us by the privacy commissioner. She is the most knowledgeable person on this issue in the province of Ontario and we need the time, as legislators, to get it right.

The Vice-Chair (Mr. David Orazietti): Further debate?

Mrs. Carol Mitchell: The specific request of the subcommittee was that the privacy commissioner be allocated an hour within the hearings and we specifically allocated an hour for the presentation and for rotation of questions. That was the recommendation coming forward and I just wanted to state for the record that was clearly the discussion that happened at the subcommittee.

The Chair (Mr. David Orazietti): I think the point on the issue has been made. You have a motion on the floor—

Mr. Gilles Bisson: I disagree, because I was there, and I know darn well what was said.

Mrs. Carol Mitchell: As was I. You voted on it.

Interjections.

The Chair (Mr. David Orazietti): Committee, the question has been put.

All in favour of having the commissioner come back?

Mr. Gilles Bisson: Recorded vote.

Ayes

Bisson.

Nays

Bailey, Brown, Brownell, Kular, Mauro, Mitchell.

The Vice-Chair (Mr. David Orazietti): The motion is lost.

We're going to continue with the five minutes of questions for the Liberal caucus. Proceed, Mr. Mauro.

Mr. Bill Mauro: Thank you very much for the presentation. Just quickly, because another member has a question for you as well, I want to confirm a couple of things.

One, you stated in your remarks that you're not opposed to the RFID technology. We already know that people who are interested in the EDL would do so on a completely voluntary basis. So I guess they would be aware through the process what it was they were entering into.

Given the technology, I'm not completely following what you're suggesting is the privacy risk, as you described it. As I understand it, once the embedded chip is pinged, it wakes up and transmits data. The data that's transmitted is simply a unique identifier, so if anybody was scanning the card—if it didn't fit in the slot and it wasn't in the wallet or any of that—what the illegal scanning would get would be the unique identifier number only. I'm not clear, especially when you went further in your example. You talked about the video camera and the encryption being such that it would only show the background and not the face. I'm making a bit of an analogy here. The person who scanned my chip illegally, what is it that they would be getting specifically, unless they have access to this database, that concerns you? That's specifically my question. It seems to me you're making a bit of a jump.

Dr. Ann Cavoukian: It is a jump. You're right, it is a jump, because then you have to have the number, and then you have to access the database. We're talking—

Mr. Bill Mauro: Exactly. So this is a border services database; that's the piece I need closed for me here.

Dr. Ann Cavoukian: I should have brought an example with me. Just last week or the week before—is it the Mifare?—an RFID chip was hacked.

Mr. Bill Mauro: Which chip, I'm sorry?

Dr. Ann Cavoukian: Is it called Mifare?

Ms. Michelle Chibba: Mifare.

Dr. Ann Cavoukian: There's an RFID chip called Mifare, and it was hacked, meaning that the database the information pointed to was hacked into. I can give you an example of that. Yes, this is done in an unauthorized way; there would be hacking involved. But what I'm saying is that is not as difficult as you might think. I have no idea how to do it, but—

Mr. Bill Mauro: Okay, but the—

Dr. Ann Cavoukian: If I could just finish. The technology experts who are out there are the ones saying the hackability of this information is high. This is not difficult to do.

Mr. Bill Mauro: So with respect, then, you're suggesting that the database that these people with my number could hack into is a federal American government border services database? Because that's what I think you're saying.

Dr. Ann Cavoukian: It's a Canadian database, and my colleague has been—

Mr. Bill Mauro: If I'm trying to get into the American side, I'm being—this is coming back.

Dr. Ann Cavoukian: Coming back, it pings the Canadian information because your information as a Canadian resides in the Canadian database, and the American border crossing people want to access the Canadian database.

Mr. Bill Mauro: So you're saying those federal government databases—I would suspect somebody could hack that now, whether or not they have my unique identifier number, so I'm not sure how in any way we would be changing that.

Mr. Ken Anderson: I'll just build a scenario for you. People come to our office quite a bit to talk about ID theft. What has happened, and I think the commissioner alluded to this, is that with ID theft, more and more the issue has become that organized crime is involved. What they need to do is build up a whole series of profiles for various bad consequences.

Normally, you may have persons in Ontario who protect their driver's licence, they're very careful with their credit cards, and they don't give out information. They apply for this driver's licence, they go up to the border, and the Canadian Border Services and the Ministry of Transportation in Ontario are working very hard to keep that protected. But away from the border, if the card is not protected, you can have these hackers who are purposely going in, getting the number to go off to the database—which actually resides in Ottawa, not in the States—and it has all of this driver's information. They bring up the information, and they set up cards and passports and other identification which are clones, so the commissioner referred to cloning.

1540

Mr. Bill Mauro: So they can hack the databases—

Mr. Ken Anderson: And then they can hack these databases. What you don't want is all of this extra ID.

Mr. Bill Mauro: With or without this number, though?

Mr. Ken Anderson: Yeah.

Dr Ann Cavoukian: If I could just add one other comment, the other concern is also with the tracking and surveillance capacity of the RFID. My colleague

Michelle Chibba is going to speak to the tracking capacity.

The Vice-Chair (Mr. David Orazietti): We have about a minute. Mrs. Mitchell would like to ask her question, so if you could—

Dr. Ann Cavoukian: Oh, okay. Tracking and surveillance, remember that as well—very important.

Mrs. Carol Mitchell: You talked about the consultation that you went through with the tourism industry. You heard their concerns. You know what this is trying to address. What I need to hear from you is, how commercially viable is it? What you've talked about today was, from MIT, a patent, a prototype; it's promising technology. That is a long way away from commercialization, and I'm sure you heard from the tourism industry how we need to move forward. This is something that homeland security is asking this has to be a part of—if it is not a part of it, then therefore it is no solution in their minds.

I guess what I'm saying is, we know how slow things can turn, so do you have an estimated time that it would take for it to become more than a prototype?

Dr. Ann Cavoukian: First of all, you're absolutely right: That is a prototype, and that is probably the least advanced one. I'm not suggesting that we hold up development of the EDL, which is being widely sought-after by the border communities. So I am not proposing stopping it.

What I'm proposing is continuing to do our work with the second company that I mentioned, Peratech, out of the UK. Theirs is not a proof of concept; theirs is here right now. It is being manufactured in their factories in the UK. It is a commercially viable technology. They could work with G&D, our vendor, and make this happen, not in time for the June rollout but for our rollout in another year, for example, the second iteration of the card. Not only is it commercially viable, we could make history in Ontario by developing this card with an on/off switch. It has not been done widely, so imagine if we produce this EDL in Ontario with this on-off switch for the first time ever and we sing its praises around the world. Not only would it be commercially viable, we would create a market need because everyone around the world is grappling with these problems about RFIDs; everyone has these issues. We could wave around this amazingly successful EDL with this on/off switch. We'd be making history and you would get a great, commercially viable product.

The Vice-Chair (Mr. David Orazietti): And on that note, thank you very much for being here today and for your presentation.

Interjection.

Dr. Ann Cavoukian: No, I did answer; how did I not answer your question? You said, "How is it commercially viable?"

The Vice-Chair (Mr. David Orazietti): I'm sorry; the time for questions is completed.

Interjections.

The Vice-Chair (Mr. David Orazietti): Thank you very much.

COUNCIL OF CANADIANS, ONTARIO-QUEBEC REGIONAL OFFICE

The Vice-Chair (Mr. David Orazietti): Next we have a presentation by the Council of Canadians, Ontario-Quebec regional office, Stuart Trew. If you'd state your name for the purposes of Hansard, you have about 15 minutes for your presentation. Any time that you do not use for your presentation will be divided equally among the caucuses for questions. You can start when you're ready.

Mr. Stuart Trew: First of all, thank you very much to the committee for hearing from the Council of Canadians on this issue. Before I start, I just wanted to emphasize that the council is not opposed to the entire Photo Card Act; in fact, as you'll probably hear from the representative of the advocates for the equality of blind Canadians later, having a photo card that acts as an official ID for people who don't necessarily drive is quite useful and we completely support that. We are opposed to the enhanced driver's license and the enhanced photo card that is also a part of this legislation.

Founded in 1985, the Council of Canadians is Canada's largest citizens' organization, with about 60,000 members and over 70 volunteer chapters across the country. We work to protect Canadian independence and strengthen local, provincial and national democracy by promoting progressive policies on fair trade, clean water, energy security, public health care and other issues of social and economic concern to Canadians. Much of our work falls under the umbrella of warning Canadians about the perils of deeper economic and security integration with the United States, and it is through this lens that I wish to approach our significant concerns with the proposed enhanced driver's licence in Ontario and across the country.

Despite the lack of a national discussion on new security technologies and an overwhelming rejection of the idea of a national ID card after it was proposed by the Chrétien government in 2002, the current Conservative government is encouraging provinces to create the so-called enhanced drivers' licences—EDLs—as an alternative to passports for crossing the Canada-US border. These new licences would contain biometric information such as a person's nationality, new security features like a barcode for proximity scans, facial recognition technology and a radio frequency identification chip that can be read by border agents at a distance of at least 10 metres. The new technology is being created to satisfy unilateral US demands in the western hemisphere travel initiative that anyone entering the country after June 2009 have a valid passport or some other secure document to prove nationality.

The Canadian government and the provinces are selling the EDL as a convenient way to get across the border quickly for those who might not want to buy a passport, although it should be emphasized that the proposed cost of Ontario's EDL—$75—is only $12 less than what a Canadian passport currently costs, and that

the federal government will be enhancing passports and extending their life from five to 10 years very shortly.

So far, British Columbia, Alberta, Saskatchewan, Manitoba, Ontario and Quebec have all announced enhanced driver's licence projects. The Atlantic provinces, it should also be noted, have decided to hold back in case the next US president decides to scrap the technology and tone down the security rhetoric coming out of his administration.

While some may see this technology as a harmless and voluntary means of crossing the border a little quicker without a passport, we see it as unnecessary, invasive and a backdoor approach to a North American ID card. EDLs will not make us safer from terrorism and they will not ease traffic flows at the border, but they will pose significant privacy concerns related to flawed technology and hazardous information-sharing agreements with the United States and other governments.

I've called this next section—just to highlight that Canada's privacy commissioners have disapproved of the EDLs. In February 2008, commenting on the EDL project in British Columbia, Canada's federal and provincial privacy commissioners issued a statement that no EDL project should proceed on a permanent basis unless all the information required from participating drivers remains in Canada. While information on individuals in Canada may cross borders, Canada's privacy laws cannot, and similar US laws only apply to US citizens.

The United States government is under no obligation to protect that information and could, if it wanted, use it to create profiles on any number of Canadians in order to restrict or more closely monitor the movement of certain people it considers threats to national security. This would likely be unconstitutional in Canada. Contrary to the assurances of the Ontario Ministry of Transportation, there is nothing that the Ontario or federal governments can do to make sure that US security agencies do not collect and store our personal information on independent databases. We can have a database in Ottawa, but information is information; it can be held anywhere.

We know that despite public opposition, the US government continues to work towards a system where various unrelated databases can be linked in order to mine for certain behaviours and to risk-score travellers based on various expanding criteria. Since it will be even harder to challenge your US score than it would be to challenge your score in Canada, why should we be making it easier for the US government to set up such a system on a North American scale when a passport will do the trick?

"Voluntary now" does not mean "voluntary later." Clearly, the usefulness of EDLs depends on their widespread use. For instance, if you're in a car with four friends and two of you have an EDL, you're still going to have to stop and the other two are going to have to get checked out. The Department of Homeland Security has already said that it wants to expand its own EDL program, which comes under the auspices of the REAL ID Act, which forces all US states to develop compatible drivers' licences and create linkable databases containing the personal information of cardholders. This is the template for the Canadian version.

1550

Currently, US EDLs will be used to board federally regulated airlines and enter federal buildings. We don't know how the system will be expanded, but one can easily imagine other situations where state agencies will find it irresistibly easier to scan a driver's licence for instant access to a person's profile. This is sometimes called "mission creep." Maureen Webb, human rights lawyer and activist, predicts that EDLs or other forms of biometric identification could become mandatory for travel by any means within or outside the continent, as they are becoming in Europe.

As you've heard today, the Department of Public Safety is working with the provinces and the US Department of Homeland Security to set common standards for the various provincial ID cards being planned. Documents acquired through access to information requests in the United States show that bilateral discussions related to a "one card" solution to travel security were being held through the Security and Prosperity Partnership as early as 2005, and such a card is clearly in the spirit of the 2001 Smart Border Declaration and Action Plan.

Neither the 2005 SPP nor the 2001 smart border agreement was debated by the Canadian or American electorates or voted on by our politicians. As Roch Tassé of the International Civil Liberties Monitoring Group has said, the provincial EDLs appear to be "a classic case of 'policy laundry,'" where the provinces are being asked to introduce measures that the federal government could not when it failed to secure support for a national ID card. More than this, the EDLs appear to be a way to sneak a North American ID card past Canadians, who clearly voiced their opposition to a national ID card in the recent past.

As we've heard today—we've learned it from the privacy commissioner—there are significant privacy concerns with the RFID chips, which can be surreptitiously scanned by anyone with a device capable of reading the signal at a distance upwards of 10 metres. At the request of the Department of Homeland Security, Ontario and the other provinces are adopting the passive UHF EPC Gen 2 tag, which is always sending unless it's inside a protective case, instead of a more secure document that could only be read at a proximity scanner closer to the border.

As privacy expert and University of Toronto professor Andrew Clement has said, the onus must be on the government to protect all private information it gathers on its citizens, including the unique RFID number, which does count as personal information, and not on citizens to remember to cover their cards once they have been scanned by border agents. It is conceivable that surreptitious RFID scans could occur outside the border region—in malls, banks and other public spaces—linking the unique number to other activities without the cardholder's knowledge.

There are also issues with the facial recognition technology, which is unreliable and could produce thousands of false positives at the border. Even with an error rate of 1% or 2%, the number of Canadians who could be pulled aside and harassed by US or Canadian officials who have mistaken them for a terrorist, criminal or other person of interest is enormous and will certainly lead to increased delays at the border, especially considering that there are over one million names on the current US terrorist watch list.

The potential for abuse of this system, I believe, is very high also. Voluntary or not, EDLs, like the Nexus card, which is reserved for trusted, high-value customers to the United States or Canada, will potentially stratify mobility rights along racial or class lines. Already the border has become a source of racial profiling as people from certain countries deemed high risk by the US government are harassed with little or no evidence to suspect them of wrongdoing. Not having an EDL or a new enhanced ID card proposed by Ontario could automatically make you a target for extra searches or questioning. "If you're in the slow lane, you must be trying to hide something," or so some border agents might think.

There is also new room for abuse, in that regular driver's licences will now include a person's nationality in a security environment that treats certain foreign nationals as automatically suspicious. Studies have proven that some police forces in Canada practise racial profiling. Displaying nationality on a card that should only explain that you have the right to drive and are a permanent resident of the province opens up the possibility of regular police officers acting on hunches that could have no basis in reality and, in a sense, turning them into volunteer border and immigration agents without the corresponding mandate.

Canadians need a say in this proposed EDL. While the United States government, according to the norms of international relations, has every right to restrict who can and cannot enter its territory, Canada and the Ontario government should not be going out of their way to help establish integrated North American systems that threaten our privacy for nominal or no extra security value. Federal privacy commissioner Jennifer Stoddart said this year that EDLs "may be an attempt to encourage us to harmonize with them," meaning the United States, and "we think it's unnecessary. We think it's intrusive, and we think it's a route that Canadians don't need to follow."

The Council of Canadians agrees with Ms. Stoddart. At the very least, Canada needs a chance to debate this new technology broadly before any province, including Ontario, can implement it at the border. We have the chance to put the brakes on this process of security integration or harmonization, which is said to ease the flow of goods and people across borders, but at potentially enormous costs to the privacy and real security of Canadians.

That's the end of my presentation. I'd also like to mention that I'm one of several presenters today who do in fact completely oppose the EDL, the enhanced driver's licence, as it has been proposed, and you're going to hear from more of them later. Thank you.

The Acting Chair (Mr. Jim Brownell): Thank you for your deputation. We have about three minutes, one minute for each. Mr. Bisson?

Mr. Gilles Bisson: You've answered my first question. You're saying I should vote opposed to this legislation. But I want to get to the second question. You talked about the photo technology as open and prone to problems. Either they were not able to make a match, which may slow down the process of the person crossing the border, or quite frankly identify the person wrongly. Any evidence to that effect that you can provide us with?

Mr. Stuart Trew: I'd like to defer that question, if you don't mind, to a speaker coming up, Andrew Clement, who has more information on this side of things than I do.

Mr. Gilles Bisson: Okay. Thank you.

The Acting Chair (Mr. Jim Brownell): Mr. Brown?

Mr. Michael A. Brown: Thank you. I appreciate you coming today. I guess what you're suggesting, then, is that Canadians use passports at the American border and Americans use passports at the Canadian border. One of the huge problems we have here is that Americans will be able to come into Canada without a passport, because we don't require it; however, they would not be able to get back into their own country without the passport, which many of us would think is a huge impediment to trade and to commerce and to tourism. I look across at my friend Mr. Bailey from Sarnia, where I was originally from, and we know the importance of the border there.

So if that's the case, that we would be discouraging our American visitors from coming and doing business in Canada, spending their money at our many attractions, doing those kinds of things, and knowing that the American public—

The Acting Chair (Mr. Jim Brownell): It's one minute for a question and answer.

Mr. Michael A. Brown: —doesn't have the—thanks, Mr. Chair—propensity to get passports the way Canadians do, what would you say to those people who have those concerns?

The Acting Chair (Mr. Jim Brownell): You'll have to be very quick.

Mr. Stuart Trew: Sure. First of all, there is a lot of opposition in the United States to these EDLs as well. And also, it really is the personal responsibility of those Americans coming up to Canada knowing that the law is to get a passport, I would say.

The Acting Chair (Mr. Jim Brownell): Mr. Bailey?

Mr. Robert Bailey: I'd like to second the comments of my colleague Mr. Brown. Yes, trade is important to Sarnia–Lambton. What do you say to those merchants in my riding, and I'm sure a number of other border city ridings, who are concerned with trade? I've been told by them that they're in favour of this, with the caveat that they want to know there is security. It's all right to be opposed to something like this, but what do we do in return for the economy, to improve the economy?

The Acting Chair (Mr. Jim Brownell): Ten seconds.

Mr. Stuart Trew: Again, I think I'd say that really the argument is the same on both sides of the border. The passport, it sounds—hearing from the privacy commissioner, it's going to be just as hard or possibly harder to get one of these enhanced driver's licences as it is a passport and they cost virtually the same amount of money. The argument for getting a passport is the same on both sides of the border. We don't need a new technology—

The Acting Chair (Mr. Jim Brownell): Thank you. We do have to cut it at that. Thank you for your deputation.

ANDREW CLEMENT

The Acting Chair (Mr. Jim Brownell): We'll move on, and next we have Andrew Clement. If, when you come to sit, you could state your name for Hansard, I would appreciate that. You'll have 15 minutes for your deputation. If there's any time remaining in that 15 minutes, we'll share the time.

Dr. Andrew Clement: Thank you. I'm Andrew Clement, and I'm a professor in the faculty of information at the University of Toronto, where I coordinate the information policy research program, and I'm the co-founder of the identity, privacy and security initiative there.

I very much appreciate this opportunity to appear before you concerning a topic that raises some thorny technology and policy issues. I'm speaking as an individual citizen and researcher in the area of privacy and security, and not on behalf of any group or organization.

1600

Identity documentation is playing an increasingly important role in everyday life. When there's a proposal to change a key identity document—and the driver's licence is the one that is used most often by people—it demands very careful scrutiny and wide consultation before changes are implemented, because it can affect many people's lives.

On first appearance, the Photo Card Act may appear straightforward, even innocuous. Improving the screening process to reduce fraudulent acquisition, offering a cheaper, more convenient alternative to a passport for entering the US and enabling those without driver's licences to obtain official ID are all worthy and well-supported goals. Anything I say here is not intended to detract from those points.

However, looking more closely at the specific changes proposed to the driver's licence, especially in light of the growing push to develop national ID schemes around the world and their linkages with the expansion of surveillance practices, reveals serious flaws that urgently need to be corrected before the Ontario government proceeds with its implementation.

I'll consider just two especially troublesome ID changes proposed by the act: using biometric screening and incorporating an RFID chip in the enhanced driver's licence.

First, biometric screening: Photo comparison technology, as mentioned in the act, but much better and more accurately known as facial recognition technology, is a form of biometrics widely regarded as raising serious privacy concerns. Given the state of the art and the large size of the proposed database—8.5 million registrants—there are likely to be many false matches produced automatically, which will considerably add to the cost of further screening and, more seriously, will identify as suspect significant numbers of people who will be at the very least disadvantaged and may be harmed quite seriously if they get mistaken for someone else.

Furthermore, with this population-wide database, there will be a very strong temptation to use it routinely for other kinds of identification and surveillance. A clear assessment of the risks of this function creep and how to resist it needs to be done at this first stage, rather than after the capability has been established and there are fewer opportunities for public scrutiny.

Ontario's Information and Privacy Commissioner drew attention to some of these privacy risks in connection with Ontario's previous attempt to develop a biometric identity scheme when she wrote to then-Minister Tsubouchi about the Ontario smart card project. She drew attention to the need for strict conditions under which the use of biometrics should be considered and, at the minimum, it needed to meet the requirements of the Ontario Works Act, 1997.

I'll turn now to the RFID on the enhanced driver's licence. I wasn't here for the privacy commissioner's report—I was in class—but I understand that it's come up, and also the previous speaker spoke to it. So I'll trim some of my remarks.

Certainly, one of the most serious problems with EDLs is the requirement to adopt a particularly insecure form of RFID. Over stiff opposition from the smart card industry as well as other civil liberties organizations in the US, the Department of Homeland Security has insisted on a type of RFID chip that is notoriously privacy-invasive in its potential. This standard, known as the passive UHF EPC Gen 2 tag, is already widely used in the supply chain and livestock management fields. The chip on the card would hold a unique personal identification number that anybody within a range of at least 30 feet, or 10 metres, could read with commercially available equipment that you can buy relatively easily. Then, once you can do that, you can link that to other information such as a photograph that you've taken.

The privacy commissioners of Canada collectively drew attention to this immediately after BC announced it was going to develop an enhanced driver's licence, and they pointed to the problems with surreptitious location tracking and the need to protect that personal information. They called on the government to do something about that, but as far as we can see nothing has been done beyond reiterating what I think is a false and misleading claim: that the number on the EDL chip is random and meaningless and contains no personal information, and that the protective sleeve that would be issued or

available with that will prevent unauthorized reading. The protective sleeve that some jurisdictions are making available to cardholders to prevent identity theft puts the onus squarely on individuals themselves. It will also provide no protection when removed from the sleeve at just those times when it is used, such as to show your card for various purposes, making it relatively easy to capture the number and associate it with other information about that individual.

It's therefore ironic that while some jurisdictions require the disabling of similar RFIDs in consumer items at the point of purchase, there appears to be no effective way for individuals to do likewise with a card that many of us will carry all the time. There's been no visible progress in developing less invasive features, in Canada anyway, such as a switch that the privacy commissioner referred to earlier.

That the Department of Homeland Security and apparently our own government are adamant about deploying these vicinity RFIDs when there are other options available to adopt even the obvious protective measures invites the conclusion that there are wider surveillance purposes intended here.

With earlier attempts at developing national ID schemes in Canada and the US having been thwarted in part by popular opposition, the current push for EDLs appears to be a soft-sell, backdoor approach towards national ID schemes that are harmonized across all of North America. Department of Homeland Security Secretary Michael Chertoff has been clear in his pursuit of a national ID. The Real ID Act is widely seen as a major step in that direction. It has provoked a storm of opposition: 19 states have already declared their refusal to go along with it. The EDL, as mentioned previously, is very similar to Real ID requirements in design and implementation, and the Department of Homeland Security has been working to make them interoperable. Indeed, Secretary Chertoff has noted, in referring to the EDL, that "it's kind of a Real ID with an additional feature ... a chip."

With so much fuss south of the border, it's disturbing that Canadian governments are quietly accepting these controversial ID measures. That there is so little public discussion here about the rationales and risks serves Ontarians poorly. However, once people come to understand what's at stake, I expect we'll hear more and louder voices of concern.

In short, in the name of thrift and convenience, Canadian governments are opening the door to a privacy-threatening ID scheme imposed by the US that Canadians will rightly object to once they learn more about it.

Until these issues have been addressed satisfactorily, Canadians who value privacy, national sovereignty and good governance would be well advised to get a passport instead, and our governments should help them get one.

In summarizing those concerns, I'd like to draw the committee's attention to a so-called four-part test that the federal privacy commission developed several years ago, based on the Oakes constitutional case for assessing proposed measures. In short, the four-part test states that the burden of proof should be on those who claim that some new intrusion or limitation on privacy is necessary, and that any proposed measure must meet the tests of necessity, effectiveness—that they be necessary, effective, proportionate—and intrusiveness.

In both the cases of the use of facial recognition technologies and the RFID chip on cards, I'd say that they fail to meet the test. From public information, certainly the biometric one has not done that yet; maybe it will. In the case of the RFID chip, unless there's a dramatic change in technology and policy from the United States, I can't see how it would possibly meet the four-part test.

To conclude, I would urge the committee to treat the three main changes to the ID that are reflected in the Photo Card Act separately. In particular, I'd suggest that the committee use the four-part test based on Oakes to assess the RFID and biometric capability. Unless high standards of privacy protection for the proposed photo cards can be met, this legislation should not proceed.

Furthermore, I think the Ontario government should facilitate Ontarians acquiring Canadian passports to travel to the US by reducing their cost and speeding their issuing.

The biometric aspects of the photo card should at least meet the minimum requirements of the Ontario Works Act, 1997.

Further, no more personal information should be provided to US authorities about Canadians crossing the border with an enhanced ID document, if one is passed, than is provided when using a passport. There should be full public disclosure and transparency of all the key aspects of the photo card development, issuing and operation, especially its financial costs, which may be significant, and the privacy risks, which are clearly evident.

1610

The Ontario government should clearly explain how it would substantively prevent the function creep that can easily accompany the introduction of biometric screening and enhanced ID documents.

And finally, before pursuing further ID initiatives which will inevitably come along, the Ontario government should engage Ontarians in an informed public discussion of the financial, privacy, identity and security risks, protections and alternatives.

Thank you very much.

The Vice-Chair (Mr. David Orazietti): Thank you very much for your presentation. We have about a minute for each caucus, so if we can do that quickly we can get through it. Go ahead, Mr. Mauro.

Mr. Bill Mauro: Professor, thank you for being here today. I believe you said something about how people are being misled in that the embedded chip on the card has the potential to release more personal information than we're being told. Can you elaborate on that?

Dr. Andrew Clement: Yes. I made that in reference to both the number on the chip and also in relation to the protective sleeve. In terms of the number on the card,

they've said that this is a meaningless number and that there's no way you can associate that with the person. But it's in some ways no more meaningless than your credit card number or the IP address on your computer because under situations of use—when you present it or when there's a photograph that can be taken while that card number is being read—it can be relatively easily associated with you. By standard definitions that are adopted by privacy commissions, that would be treated as personal information because it is permanent and it is unique; there's no other number that's the same and it's associated with your person.

Mr. Bill Mauro: But in practical terms, how would somebody, if they had my number somehow, know that it was associated with me, unless they were able to get into the database that it links to?

Dr. Andrew Clement: If you take your card out, let's say, when you're buying something or you have to show it, like at the post office or something, then they can read the number off your card and they can take a photograph of you.

Mr. Bill Mauro: They can read the number off my card?

Dr. Andrew Clement: The reading of the number on the card can be done at a range of 30 feet. So if I had the equipment, I could bring it into this room and read the card numbers of all of the cards of everybody in this room that were not protected.

Mr. Bill Mauro: Thank you.

Dr. Andrew Clement: That's been designed as a feature of this so that they can put the readers across the roadways, so they can read it under rather difficult circumstances.

The Vice-Chair (Mr. David Orazietti): Thank you. Mr. Klees.

Mr. Frank Klees: Thank you, Professor Clement, for your presentation. The privacy commissioner in her presentation referred to a technology that could actually switch these cards off. You're familiar with that technology?

Dr. Andrew Clement: Yes. I have recommended that as a possibility.

Mr. Frank Klees: She suggested and was pretty excited about the fact that that technology is real and could in fact be implemented into the Ontario project. Given that, is your concern regarding the EDL chips then addressed, or do you still have concerns?

Dr. Andrew Clement: There are quite a number of problems with the EDL chip, but the on/off switch would help greatly. I guess I differ with the commissioner when she says that you should go ahead with the existing implementation and then bring in the more advanced one later. I would suggest that we not implement the current version because it is dangerous for the reasons we've elaborated, and that when other forms of identification are needed—where the case has been made for the need for good identification—then an on/off switch would be very helpful. So I would see that as a good move, but I don't see that it's appropriate in our circumstances yet.

Mr. Frank Klees: Thank you.

The Vice-Chair (Mr. David Orazietti): Thank you very much for your presentation.

GS1 CANADA

The Vice-Chair (Mr. David Orazietti): Next we have GS1 Canada. Eileen Mac Donald and Kevin Dean are here. Welcome. You have 15 minutes for your presentation. Any time that you do not use during your presentation will be divided among the caucuses for questions. Proceed when you're ready. Please state your name for the purposes of Hansard.

Ms. Eileen Mac Donald: My name is Eileen Mac Donald.

Mr. Kevin Dean: Kevin Dean.

Ms. Eileen Mac Donald: Thank you for the opportunity to present to you today with respect to the public hearing on Bill 85. Kevin Dean will be here to answer any technical questions with respect to what I'm about to communicate to you.

What I want to do, first of all, is give you a brief overview of GS1 Canada and why it's important that we're here today. GS1 Canada stands for global standards, and we are a member organization of GS1 globally. There are over 145 countries that are GS1 countries; I think that's very important to note. Our first and foremost mandate is to represent Canada in the development of global standards. So we will sit at the global table when a standard is being developed and we will identify the Canadian requirements, and we ensure that they are baked into the standard, such as building codes, metric, bilingualism, etc.

As the Canadian member of the global GS1 organization, our role is not only to ensure from a standards perspective, but the governance model is to ensure that companies of all scales are able to partake in the standard that's being developed. We are known for building communities of interest around a standard, such as the electronic product code which is currently embedded into the EDL, which is very important and why we're here today. We would have represented Canada in the development of that standard over the last five years; I think that's important to note. We have 25,000 members and 80% of those members are small companies.

I think it's very important, before I continue, that it's understood that we are not a solution provider. We do not engage from a technological perspective. Our first and foremost mandate is standards. Secondly, what we do is education, and we also offer implementation services from time to time to help a specific industry upon their request.

Our role is to represent Canada in the development of standards. I think it's very important to make sure that that's understood. I'm repeating myself.

I think it's important to understand that EPCglobal Canada is an affiliate of GS1 Canada. We purchased the MID technology. What you would know us mostly for would be the bar code. We implemented the bar code in

Canada, and from a global perspective there are over five billion transactions on a daily basis of this particular standard. GS1 Canada manages the mandate wholly, which is the subsidiary of EPCglobal Canada. We believe that the electronic product code is moving forward in being the next generation of the bar code, with the usage of radio frequency identification.

GS1 Canada first became involved in the provincial EDL initiative in 2007, in the early stage of governments planning with respect to processes. As you know, in response to the US western hemisphere travel initiative, the governments of the United States and Canada agreed to accept an optional enhanced driver's licence as an alternative to passports going over the border.

The US Department of Homeland Security has determined that the EDL will be the vicinity RFID-enabled card. You would know from a technological perspective, as it relates to RFID technology, it's been around for a long time. In many cases, your pass card would be RFID technology. That would not necessarily be a global standard. The EPC chip or the RFID code built into the driver's licence would be based on a global standard for the purposes of interoperability.

Homeland Security selected the vicinity RFID for the EDLs as a means of speeding travel time across the border. In 2007, Homeland Security and the Canada Border Services Agency selected GS1 standard, which would be the EPC code, for the RFID technology and the document identification for integration into the enhanced driver's licence, as they enable the requirement for vicinity RFID while safeguarding sensitive personal information. GS1 standards do not include any personal identification information. This is a very important component. So right now, if I go over the border—and I travel a great deal—I give you my passport as I go through from a flight perspective and they're scanning it, there's a lot more information there than there is with respect to the driver's licence. I think that's important to note. Similar to the licence plate, when I go through the border and I'm driving over they're tracking the licence plate right now, which would then ultimately tie back to the individual owning the car.

1620

Similar to the licence plate, this unique document identification number is transmitted to a government computer system and is used as a pointer to the location in the secure database where this information is stored. The importance of the use of the global standards in Canada in the Canadian and American enhanced driver's licence initiative cannot be understated. It's very important not to use proprietary systems. That's where you run into a lot of the concerns which are warranted. Privacy and security requirements are built into the design of the GS1 standards. So when I speak to you about the communities' interest, our role is to bring all of the appropriate players to the table to identify the requirements, from beginning to end, for the purposes of implementation. So to have an understanding of the importance of privacy, and within what we're working on within Canada, we've engaged with four privacy commissioners with respect to this initiative.

Standards are the foundation for clear, consistent and understandable exchanges between parties. In the case of the enhanced driver's licence, this means that each province captures and encodes the driver's licence information in the same way, ensuring the same technology requirements at every border crossing across the country for reading and interpreting information. More broadly, GS1 standards can also facilitate faster cross-border identification of products in areas such as customs programs, product traceability, anti-counterfeit, logistics efficiency and regulatory compliance.

We are also engaged right now. GS1, from a global perspective, has a memorandum of understanding with the World Customs Organization and CBSA to advance these specific types of initiatives. Thus, as the government of Ontario advances Bill 85, the integration of the GS1 standards into the EDLs will also support other governments' measures for ensuring efficiency, effective flow of goods, people and information across jurisdictions.

Here are our recommendations, based on our experience with BC and with Washington:

—that the government legislate against deliberate scanning of the card for unapproved purposes;

—that the enhanced driver's licence be issued with a protective sleeve—and, yes, the commissioner was correct that there is a capability of an on/off switch;

—that the EDL be locked, using built-in security features to prevent re-writing of the card, such as denial-of-service attack;

—that the EDL's serial number be random and that this serial number be changed whenever the EDL is renewed;

—that the government provide a comprehensive public education site, similar to that provided by Washington state; and finally

—that the government work with GS1 Canada to help ensure the application of the standard-based processes and best practices for security and privacy and to help enable standard-based interoperability between Canada and the US.

When we talk about the applications and the standards, you will see through the pilots that any of the issues were when you went outside of the standards. So the users and the technology all need to be certified with respect to ensuring they're respecting the standards.

I thank you.

The Vice-Chair (Mr. David Orazietti): Thank you very much for your presentation.

We have just about a minute for each caucus as well. So if Mr. Klees would like to start, if he has any questions. I'll start with you this round; thank you.

Mr. Frank Klees: You're obviously familiar, then, with the various companies and their technologies worldwide that deal in this technology. You heard the commissioner's comments about the on/off switch technology

and so on. Could you just comment on the reliability of that technology? What experience do you have with it?

Mr. Kevin Dean: The on/off switch?

Mr. Frank Klees: Yes.

Mr. Kevin Dean: It's like the on/off switch for the microphone. The microphone has the capability of recording everything I say, but there's somebody who is controlling the switch. The RFID chip is a circuit just like any other and if the switch is not turned on, the circuit won't activate no matter what you do with it.

Mr. Frank Klees: And that technology is now commercialized, is it?

Mr. Kevin Dean: Yes. It's a trivial addition to an RFID chip.

Mr. Frank Klees: Where is it being used?

Mr. Kevin Dean: The company that the privacy commissioner mentioned is not one that I'm familiar with, but we do know that IBM, for example, has removable and replaceable tear-off strips on their tags to protect the RFID information for similar purposes in shopping applications.

The Vice-Chair (Mr. David Orazietti): Mr. Bisson?

Mr. Gilles Bisson: Just a question. You make a recommendation to make the serial number on the EDL completely random. Explain that. If you make it completely random, how do they read it? I'm not quite sure of the technology.

Mr. Kevin Dean: It's not random every time you read it. You still read back the same number, but rather than assign serial number 1 to me, 2, 3, 4, 5, 6 and get a sequential, easily guessed sequence of numbers, you assign 1, 2, 3, 4 to me, 7, 8, 3, 1 to you, and so on down the line. None of these numbers are in any way related to each other. There's no known sequence to them, so it's not possible to create an EDL chip with a number that might be valid.

Mr. Gilles Bisson: Is there any technology to stop the deliberate scanning of cards? You're saying legislate it, but if you legislate it, somebody will break the law. Is there a way of denying that type of access?

Mr. Kevin Dean: No more than there is to prevent somebody from taking a photograph of my licence plate and recording my location at the Legislature building today.

The Vice-Chair (Mr. David Orazietti): Mr. Brown?

Mr. Michael A. Brown: I, too, am intrigued by the on/off switch and the commercialization of that technology. I think we would all agree that is a good thing to be doing, if we possibly could do it in the time frame we have allotted. I would just ask that you help us out and provide us with the kind of information that the government would like and the opposition parties would like so that we might have a look at how that might be implemented.

Mr. Kevin Dean: We would certainly be happy to do so. We work with a number of companies in their implementations of RFID in a variety of ways.

Mr. Michael A. Brown: Thank you. We appreciate your expertise.

Mr. Frank Klees: Chair, if I might then, with regard to the undertaking, could we ensure that information is distributed to members of the committee when received, and could someone follow up with them on that?

The Vice-Chair (Mr. David Orazietti): We'll ensure that the information gets to the clerk and that it's sent to all members of the committee.

Thank you. That concludes the time for your presentation. Thank you for being here today.

CANADIAN CIVIL LIBERTIES ASSOCIATION

The Vice-Chair (Mr. David Orazietti): Our next presenter is the Canadian Civil Liberties Association, if I could call on Graeme Norton to come forward, please. Thank you very much for being here today, Mr. Norton. Please state your name for the purposes of Hansard before you begin and then you have 15 minutes for your presentation. Any time that you do not use will be divided up for the caucuses to ask questions of you. So go ahead whenever you're ready.

Mr. Graeme Norton: Certainly. Thank you. My name is Graeme Norton and I'm here with the Canadian Civil Liberties Association. I'd like to thank the committee for giving us the opportunity to appear before you today on this important piece of legislation.

Like many of the others, we don't take issue with the objectives of this legislation. Obviously promoting tourism and trade, and finding ways for that to happen more easily, is a desirable objective and relatively benign. What we take issue with is the means that have been used to achieve those objectives. We think that those means have the potential to threaten privacy and civil liberties in substantial and significant ways and we think the challenge before the committee in dealing with this legislation is to find a way to achieve the desirable objectives of the legislation without unnecessarily intruding upon civil liberties and privacy rights.

I have the fortunate position of going at the end of some of the presenters, so I will not walk you through some of the specifics of the technologies in the way that some of the parties that have gone before me have been kind enough to do. So I will try to proceed with our recommendations, discussing briefly the technologies to the extent necessary as we go.

Like many of the other presenters here today, the Canadian Civil Liberties Association is very concerned about the privacy and civil liberties threats posed by Bill 85. In our view, it is inappropriate to introduce photo comparison technology and RFID-equipped EDLs into Ontario's driver's licence regime. These technological powers are not proportional to their objectives and have the potential to significantly threaten privacy and civil liberties. The potential for function creep with these technologies is very real and we don't feel that this is a fact that Bill 85 sufficiently addresses. In our written submission, we set out a series of recommendations with

respect to the bill that we urge you to consider in your deliberations about this legislation.

1630

On the issue of photo-comparison technology, the CCLA is concerned that the bill does not sufficiently circumscribe how the technology can be used. As noted, photo-comparison technology can and has been used for a wide range of identification purposes. In the United States, for example—and I'm not sure if anyone's mentioned this today—it has been used for surveillance purposes. At the Super Bowl in 2001, for example, all attendees were photographed, and their photographs were scanned against a database of known criminals that existed previously. It has also been used in programs where cameras have been set up to photograph people's faces as they walk down the street, and to take those photographs and use them against an existing database of photographs.

So this is a technology that has a range of potentially privacy-invasive applications. It doesn't appear that the bill is intending to employ it in this type of way, but its introduction alone is concerning to us if how it can be used is not closely circumscribed.

Furthermore, we're not convinced of the necessity of using this technology. It doesn't appear that licence fraud is a sufficiently significant problem to warrant the introduction of a technology as potentially invasive as photo-comparison technology. Moreover, it's not clear, based on its ability to actively predict whether or not an individual matches up with a picture, that it will be effective in accomplishing the objective of fraud protection for which it is implemented.

To us it's also significant that the US government does not require that this be part of an EDL. This is something that Ontario has taken on, so it's not like some of the other things, such as RFID, that are required if we want to participate in an existing program of another government. Therefore, the CCLA believes that including photo-comparison technology in the bill is not appropriate and that the provisions that enable it should be excised. In the alternative, if that's not done, at the very least we think that more substantial safeguards must be put in place in the bill in terms of how photo-comparison technology can be used. The biometric information and its underlying root images should be closely guarded and only used for highly specific purposes.

With respect to the actual text of the bill, we note that paragraph 11(4)7 allows for the disclosure of information, which appears to include information that would be used to generate photo-comparison technology imagery and the underlying biometric data to any Canadian, federal, or provincial government for a variety of purposes. One such purpose is the prevention of improper uses of photo cards. From our perspective, that's a very broad purpose, and to permit the disclosure of this type of information to any Canadian government for that broad a purpose creates the potential for a lot of unwarranted information sharing and could lead to inappropriate use of this type of data.

The CCLA is of the opinion that the sensitive nature of the biometric information that could be collected under the bill requires clearer safeguards. To this end, we would recommend several things.

We would recommend that the bill should specifically foreclose the possibility that biometric-capable data could be used for anything other than preventing people from fraudulently obtaining Ontario driver's licence and photo cards. Furthermore, as only Ontario could have a valid interest in using photo-comparison technology biometrics for this purpose, the bill should specifically prohibit transferring such data and information to other Canadian or foreign governments.

Continuing on the technological front, the CCLA, as I'm sure you won't be surprised to hear, is also deeply concerned about the use of RFID. When considering implementation of this technology, it is important to remember that EDLs and driver's licences, unlike passports, are documents that people carry with them at all times. If the type of RFID proposed is included on the licence, then licence holders, like warehouse stock, will be detectable from up to 10 metres, or more, away. That's a significant intrusion into their privacy, from our point of view. If I knew all of your underlying numbers, I could detect that you were sitting there right now if I had the correct technology to do that.

In CCLA's view, dealing with this problem by giving EDL holders a protective sleeve in which to store their licence is simply insufficient to protect against the potential privacy threats posed by the technology. We envision that such sleeves are likely to be damaged, lost, or to simply go unused, resulting in information on RFID chips being available frequently and, for some people, at all times.

Moreover, the CCLA believes that other, less intrusive means could be used to provide border officials with advance notice of who's approaching their station. One possibility that has been proposed in other jurisdictions is, instead of broadcasting the data to the border station, having a short-range reader 30 metres or 10 metres ahead—whatever the distance—where somebody could just swipe their card as they approach, thereby accomplishing the same thing, giving the border station early notice of who's approaching without having to require insecure broadcasting of that data over the airwaves.

We don't see that RFID is necessary here, and we think that it should not be included. I understand that there's the reality that the US is requiring it, so that's the difficult thing to deal with here. RFID, and a specific type of RFID, has been proposed. We would prefer that the type that has been proposed not be used. There are much more secure types. There are shorter-range chips that will not broadcast as far and can encrypt data, and we would encourage further negotiations with the Department of Homeland Security to see if they would be willing to perhaps consider a more secure chip. In the alternative, if they would push forward, we would agree that Commissioner Cavoukian and others have made good suggestions about the on/off switch potential of

other chips, which can be used to meet the US requirements. We would push for a change to the type of technology that is likely going to be used there.

We would also suggest that the bill clarify that RFID can only be accessed by border officials for the specific purpose of identifying travellers and that it should be an offence for any other person to access that information for any other reason. This has been done in other jurisdictions in the US. I'm not sure how effective that legislation has been, but having it on the books would at least provide an additional safeguard.

Finally, we would agree with previous presenters that the unique identifier contained on an EDL should not be linked to that individual forever; it should be changed at periodic intervals. For example, when you go and get a new driver's licence, you should, at a minimum, get a new unique identifier, so that somebody who may have come into contact with it would at least have to get it again.

On the issue of participant data, we have further concerns with respect to the type of information that may be transferred to American authorities under the bill. Our research indicates that US border agencies have broad powers to retain and disclose information on travellers to the US. They can hold this data for up to 75 years, apparently, and can disclose it broadly to government agencies for a wide variety of purposes. For those with EDLs, such information would appear to include a driving record, if we follow the examples set by other provinces. You could tell when somebody's licence had been suspended, and this would be information included and passed along to US authorities. We don't see any need for this. For example, we don't understand why American authorities would have to know why a passenger in a car or boat had once, in the past, had their driver's licence suspended. We simply don't think that's relevant. Going to that point, we would recommend that any information not required to determine admissibility to the US should not be passed along to American authorities under an EDL program.

Finally, given the potential for abuse of EDLs and their ongoing accompanying technologies, the CCLA believes that the introduction and ongoing use of EDLs should be subject to broad-reaching independent scrutiny. Such scrutiny should be focused on identifying potential civil liberties concerns resulting from the use of EDLs and making recommendations about how such problems can be remedied.

An independent audit body should be given the authority to scrutinize, with full access to records, facilities and personnel, the implementation and ongoing use of EDLs. Regular public reports should be submitted to the government regarding any problems—and not just to the government but to the Legislature, publicly, to clarify that point—relating to EDLs and recommending how such problems can be corrected. While the recommendations would not be binding on government, they would place pressure through the publicity that would be generated by them for the government to ensure that EDLs negatively affected civil liberties and privacy rights as little as possible.

In conclusion, the CCLA urges the committee to consider our recommendations and not to pass the bill until amendments have been made that will sufficiently curtail the significant threats to civil liberties that it could cause.

Thank you again for the opportunity to appear before you today. If you have any questions, I would be pleased to answer them now.

The Vice-Chair (Mr. David Orazietti): Thank you very much for your presentation. We'll start with Mr. Bisson. You have about a minute or so—a minute and a half.

Mr. Gilles Bisson: One of your recommendations is that you remove the photo-comparison technology from the bill. What would you do in its place? How would they be able to identify who the person is?

Mr. Graeme Norton: With respect to fraud protection?

Mr. Gilles Bisson: Yes. Well, not only fraud protection, but from the perspective of crossing the border.

Mr. Graeme Norton: From the perspective of crossing the border? I'm pretty sure that they could use whatever means are currently in place for doing that. It's not required by the US that that be part of the EDL, so I don't think that they require it as part of their access strategy. That is strictly, from my understanding, something that Ontario has decided to include in the program.

Mr. Gilles Bisson: You also said that the end-use requirement on the part of the Department of Homeland Security is that we meet a certain standard. You talked about the technology being used. Do we go to a passive system or an on/off system? If the Americans should say that they don't accept the on/off system, what would you do if you were Ontario?

1640

Mr. Graeme Norton: That would put you in the difficult position of either having to decide to abandon the legislation, effectively, or to accept the potentially threatening standard imposed by the US.

Mr. Gilles Bisson: Your recommendation?

Mr. Graeme Norton: My recommendation would be to not go forward with the bill in its current form with that standard.

The Vice-Chair (Mr. David Orazietti): Mr. Brown?

Mr. Michael A. Brown: I appreciate some of the issues that you brought forward. I think some of them we've heard for the first time, at least in this forum. My first question is, do you have any idea, where there is this on/off technology for the chip, how often people would use it versus putting it in a sleeve? I'm not very convinced that there is that much difference in terms of usage. Is there information about that available?

Mr. Graeme Norton: Yeah, I can't claim to have in-depth knowledge about that technology. I'll just make a guess at how it might work. From my experience, I was given a sleeve when I got my last bank card, and I

haven't seen it in about seven years. So that informs my opinion on the sleeve issue.

I've never had a card with an on/off switch on it. I might be more diligent with that, but I definitely see that two safeguards are better than one safeguard, as one safeguard is better than no safeguards. I'm sure that some people might still leave it on and that it wouldn't solve all problems, but it would be a step in the right direction for sure.

Mr. Michael A. Brown: To the issue of information that might be shared, it's the intention for the card not to share any more information than a passport would provide you with. Do you have any problem with the information a passport provides?

Mr. Graeme Norton: No, not per se. That concern arises from some of the information that is passed along in other jurisdictions. My understanding is that the program in BC enables further transfer of data that goes above and beyond what is currently passed along with a passport.

Mr. Michael A. Brown: I believe BC's is a relatively small pilot project—I can't remember the number, but it's relatively small—and hopefully the lessons that are learned there can be shared across the country.

The Vice-Chair (Mr. David Orazietti): Mr. Klees?

Mr. Frank Klees: Thank you for your presentation. We heard from the privacy commissioner the extent of the information that would potentially be required and it does go, in fact, far beyond what is required for passport information. Why would someone be asked to provide so much more personal information than even a passport? What could possibly be the reason, in your opinion?

Mr. Graeme Norton: Again, I'm in a position where I can make no more than a wild guess at that question.

Mr. Frank Klees: Go ahead.

Mr. Graeme Norton: I don't see any particular rationale for doing that. If, under a passport program, only a certain amount of information is required to enable you to get into pretty much every country in the world, I don't see why more information would be required as underlying information in an EDL program to get you into a country that, previously, was happy to allow people in with just a driver's licence. Again, I would agree with the privacy commissioner on that point that as little data acquired through this program as necessary would be desirable.

Mr. Frank Klees: You were very strongly opposed to photo-comparison technology. When the minister presented that, it seemed harmless, quite frankly, but you're strongly opposed to it. I'd like you to just tell us why you have such a strong opposition to photo comparison.

Mr. Graeme Norton: The way it's proposed for the detection of fraud protection or prevention of fraud with driver's licences—I really question whether or not it would be effective in achieving that, based on my understanding of its likelihood of being able to identify photographs matching up with an individual. We don't see it as necessarily required to promote that objective. If it is to be brought in, it may bring certain benefits along with it.

Our biggest concern is that it only be used for that very specific purpose if it is used. It has, as I mentioned, been used in other jurisdictions for other purposes and we would be very much opposed to that, so if it is brought in for that specific purpose, the bill should be very clear about that and foreclose the possibility that it could be used for anything other than fraud detection.

The Vice-Chair (Mr. David Orazietti): Thank you, Mr. Norton, for your presentation.

STEVE MANN

The Vice-Chair (Mr. David Orazietti): Our next presenter is Mr. Steve Mann—if you'd like to come forward, please. Welcome, Mr. Mann. You have 15 minutes for your presentation. Any time that you do not use will be divided among the parties for questions. If you'd like to state your name for Hansard and proceed when you're ready.

Dr. Steve Mann: My name is Steve Mann. Thank you for giving me the opportunity to speak here today. I'm a professor at the University of Toronto. My technology and designs—I work on electric seeing aids, computational seeing aids, devices to assist the visually impaired and visual memory aids and things like that. I build electric eyeglasses and that kind of technology, so I come to the privacy issue from a different perspective; for example, if somebody is remotely sending video and allowing somebody else to help them see better, or visual memory prosthetic and mind files and that sort of thing.

So I enter into the privacy arena from a different kind of technology—what we call "sousveillance," le contraire to surveillance. "Surveillance" in French means to watch from above. "Sur" means above, and "veiller" means to watch. "Sousveillance" means to watch from below, so sousveillance pertains to technology on people and surveillance is technology on architecture and buildings, in some sense. We work on these technologies, and we've got a community of about 30,000 cyborgs now who engage in their day-to-day lives, living online and that sort of thing.

I approach this technology from the point of view of privacy, but also one of the things that I've encountered living this life—and with the growing population of the elderly, there's going to be more and more people using electric eyeglasses and seeing aids and that sort of thing. One of the problems is that we often get harassed by security guards. Security guards are afraid of any sort of accountability sometimes, so we experience the world a little bit—see some different things that might not have been seen before.

I researched the history of terrorism, because terrorism is often the reason for a lot of these surveillance initiatives. When I did an initial study on terrorism, I found the first occurrence of the term "terrorism" was used to describe the reign of terror in the French Revolution. The word "terrorism" was first used—its original definition

was an act that a government perpetrated against its own people in order to terrorize them into submission. If you do a historical look at terror, it comes from French, much like surveillance and sousveillance are also French terminology—there's a French history. The world's first terrorist organization was the committee on public safety, COPS. It's interesting COPS was this committee on public safety. It was a government organization that was the world's first terrorist organization. So I see the world from this reversed perspective, and I can't help but question what the checks and balances are.

One of the things that this technology does, in a sense—Andrew Clement made reference to RFID being used on livestock—is make us like electronically tagged animals at feedlots. I asked myself a very simple philosophical question: What is the difference between wildlife and livestock? Wildlife crosses the border without asking permission, without showing ID, without carrying identification, whereas livestock carries identification. Wildlife is free; livestock is owned by somebody else. The question that comes into my mind is, who owns me? Do I own myself—i.e., am I wildlife? Or am I owned by somebody else, a large corporation that's making a lot of money by tracking my movements—i.e., livestock?

My concern is really not so much about hackers getting into the system, but more about the potential conflict of interest and the "enemy within" aspect of it. What will prevent it from being used to terrorize people—terrorism in the traditional sense, what it used to mean or originally meant? What prevents that form of terrorism? What sort of liability is there when individuals are targeted and harassed internally for their beliefs or their actions, or just because they're a little bit different? Even just somebody who's differently abled often becomes the victim of harassment and terrorism. I've heard just all too many situations of a deaf child being shot by police because he didn't respond to orders or a visually impaired person being attacked because he didn't see the policeman command him to do a particular thing.

1650

What are the checks and balances for all of this huge amount of surveillance? I kind of like to use the ladder analogy with surveillance. If we put cameras in the east end, it will push crime to the west, but if we put cameras in both the east end and the west end, it will push crime up the ladder of life, and those on the bottom-most rung may no longer perpetrate crime, but it will become more profitable to perpetrate corruption. In other words, the crime moves up. Surveillance tends to, by its nature, push crime upwards when it becomes pervasive. It doesn't push it east or west; it pushes it up the ladder, and the very surveillance system that was put in to protect us can be abused with its potential inherent conflict of interest. I think of a ladder as having different rungs, and the bottom rung of the ladder looks down; that's surveillance.

There's another word called "oversight." In English, "oversight" means the same thing as, in French, "surveillance." "Oversight" is a literal translation of the word "surveillance," but usually it means further up the ladder. The way we normally use the word is congressional oversight. We look down from above, higher up. So congressional oversight also looks down the ladder as well.

What mechanism is there for sousveillance and what I call "undersight," the English translation of sousveillance? Surveillance is the bottom rung of the ladder looking down, sousveillance is down at the bottom looking up, and oversight is higher up, also looking down, but undersight is sort of mid-ranks looking up. So what undersight and sousveillance mechanisms are in place for this technology? It seems like that might be something that's missing, hasn't been thought of or hasn't been considered.

There are obvious technical issues, like that Faraday cage: How many decibels of attenuation does it give? There are crazy things, like that on/off switch: Is it waterproof? Some people swim with their wallet. They just carry a few credit cards and some change or something and they don't use a wallet. They just have a little clip that holds it together. A lot of people just don't want to take it out when they go for a swim and have it stolen. So if I were to go for a swim in a saltwater ocean, what would become of that on/off switch?

But more importantly, if you think of that on/off switch on the card, if this was my card here and on the edge of it, it had this on/off switch, why not just put a couple of contacts, have the on/off switch over here and just have a card reader, and you stick it into the card reader and the on/off switch closes? Why have an RFID at all? The best on/off switch is contact closure from the card. You stick the card into some contact closure that turns it on; there's your on/off switch. The on switch is built into the card reader and you insert it. Why not just simply have contacts on the edge of the card like they do already now and that's your on/off switch? Why have the RFID at all, really? Why not just use a contact-based card-reading system, because then you'll have your on/off switch and it will be waterproof and reliable, and it's proven technology? Why advance to this increased surveillance technology?

It's not just the issue of hackers, but it's also the issue of what prevents the corruption that might follow or the abuse of it, especially when it's outside of our country. The US keeps it for 75 years, and maybe they even break the law. A lot of these higher organizations operate above the law; they don't respect the law. Why give our Canadian sovereign ID to a country that may or may not respect the law by organizations that may or may not respect the law, organizations that are above the law? Why open ourselves up to that risk?

The Vice-Chair (Mr. David Orazietti): Thank you very much for your comments. We'll start with the Liberals. You have about a minute and a half for your questions. Go ahead, Mr. Brown.

Mr. Michael A. Brown: We appreciate you being here, bringing a perspective I don't think we've heard before today, and we appreciate that.

I would bring you to the point that this is also a photo card that could be used as identification for people who aren't drivers. We've been talking here a lot about how it might be used at the border, but this is also just a regular card that can be used anywhere, which does not necessarily need to have any of the technologies or anything attached to it. You can get a photo card in this technology that just allows people to be identified. There are a number of people in our society who don't drive, for example, and therefore would not have a driver's licence, and who would find this useful. Could you comment on that?

Dr. Steve Mann: Well, sure. You can use other things, like a passport, a health card or something else. I guess my comment is, whether you drive or don't drive, that's not really the issue. The issue in my mind is whether we become electronically tagged animals at feedlots, whether we become livestock that's tracked. Whether there's a sleeve on there, and its attenuation, of course—the sleeve—gets lost or worn out or whatever, in practice, if you start tracking people like this, it sort of heads down a slippery slope.

Mr. Michael A. Brown: I understand that, but many people would choose not to have that. You can choose. This is totally voluntary. If you don't want to have this, you can have a passport. If you want to have just plain identification without any technology attached to it at all, you can.

Dr. Steve Mann: Would it be voluntary like taxation? Taxation was voluntary when it first came out. I'm worried about developing the technology, because it might start out being voluntary and then, you know—

Mr. Michael A. Brown: I take your point.

The Vice-Chair (Mr. David Orazietti): Mr. Klees.

Mr. Frank Klees: Thank you very much for your presentation—most interesting. I've heard words today I've never heard before, and thanks for explaining them. You raised—

Mr. Gilles Bisson: It's called French.

Interjections.

Mr. Frank Klees: Merci, merci.

Dr. Steve Mann: Les nouveaux mots.

Mr. Frank Klees: You used the term "slippery slope," and I think Mr. Brown believes his government, actually, when they say that this is going to be totally voluntary, and no doubt it will be at the outset. The reason that we're all so concerned about what this actually will look like, I think, is that we all believe at some point it will move beyond the voluntary stage. That's the reason we have to guard it so carefully now, because if we go down this road and we are not vigilant on these privacy issues, then we find ourselves with a lot of information out in places we don't want it to be.

I thank you for raising that concern, and we'll certainly do what we can to hold the government to account and to ensure that these privacy safeguards are in place. So thank you for your presentation today.

I have one other question for you, with your permission. I have never heard the term "electronic eyeglasses." Could you explain that for us?

Dr. Steve Mann: Hearing aids now have all gone electric, computerized, and the next-generation eyeglasses download your prescription over the Internet. When your eyes get tired or at the end of the day you get a stronger prescription automatically, or if you're reading, instead of having a little field of view, your entire field of view goes to reading. Also, we have been looking at people who are legally blind but still have some remaining eyesight being able to read, because it renders everything in laser light, so it has a clarification of things. It's something we have invented in our research lab at the University of Toronto.

Mr. Frank Klees: Wonderful. Thank you for that explanation.

The Vice-Chair (Mr. David Orazietti): Mr. Bisson.

Mr. Gilles Bisson: Maybe we should have had translation so people understood those French words. Just joking.

A really interesting presentation. I think you're at a level on this issue that most of us are not. You're looking at the whole issue of privacy from the perspective of individual rights versus the right of government to survey what we're doing, and I think it's quite interesting.

I'm a little bit puzzled, though. You're saying on the one hand that you are opposed to the RFID; rather, you want to have some sort of swipe technology with a contact system that they swipe and that makes it safe. But on the other hand, you're worried about the information that could be gathered by whomever—in this particular case, the American side of the border—and that that information could be used against you. How do you square those two things off?

Dr. Steve Mann: I guess I'm not saying that I have a full solution to it. This isn't really my area, so I don't really understand all of the issues. I'm kind of expressing my overall concerns that we are rushing into a surveillance society and a police state unnecessarily, that in some sense, because the Americans tell us that we need to crack down on terrorism, maybe we should ask them for a second, "Well, hey, wait a minute. What is terrorism?" Look, it was originally governments terrorizing their own people with excessive security.

1700

Mr. Gilles Bisson: Even France has figured it out. They're going the other way, along with Europe. They've actually lessened the restrictions on border crossings—

Dr. Steve Mann: Yes, they've opened up—

Mr. Gilles Bisson: —which is kind of interesting.

Interjection.

Mr. Gilles Bisson: Well, have you been to Europe lately? You walk into the Frankfurt airport, they don't even stamp your passport anymore.

Dr. Steve Mann: Yes. When you get to Europe, you don't even know you've cleared customs. I was walking out onto the street, and I said, "Oh, when did I clear customs?"

Mr. Gilles Bisson: Exactly. It's interesting. We've taken a completely different approach, and I think that's

the point you were making. You're saying, "Should we really be going down this route?"

Dr. Steve Mann: Yes. The world's opening up in many ways. There are all these questions about terrorist nations.

Mr. Gilles Bisson: Thank you.

The Vice-Chair (Mr. David Orazietti): Thank you, folks. That concludes the time for your presentation. Thank you very much, Mr. Mann.

ALLIANCE FOR EQUALITY OF BLIND CANADIANS, TORONTO CHAPTER

The Vice-Chair (Mr. David Orazietti): We have one more presentation: Alliance for Equality of Blind Canadians, Toronto chapter, Phil Wiseman, vice-president. Would you like to come forward? Thank you very much for being here today, Mr. Wiseman. You have 15 minutes for your presentation. Any time that you do not use in your presentation will be divided up for questions among the parties. Please state your name for the purposes of our recording Hansard, and proceed when you're ready.

Mr. Phil Wiseman: Thank you for allowing me to come and speak with you this afternoon. My name is Phil Wiseman. I am vice-president of the Toronto chapter of the Alliance for Equality of Blind Canadians. We represent a national organization of blind, deaf-blind and partially sighted Canadians and friends of the blind working together to try to enhance our rights through advocacy, public awareness and other initiatives.

Our chapter has been involved in working on lobbying the government to implement a non-driver driver's licence since 1996. We have tried a number of ways. We started a petition and collected 850 names. We managed to meet with the Minister of Transportation in 1999, when we submitted the signatures. We've tried to establish numerous contacts with the minister to try to see what we could do to expedite this. We thought that perhaps all government politicians needed to be made aware of the issue, so we embarked on a letter-writing campaign to all the MPPs, and then we did our best to make contact with as many MPPs personally in our communities. When we went out to speak in the community, we were telling people about this issue.

Before people should run into their houses and lock their doors for fear of the blind hitting the road with their guide dogs, let me assure you that won't be the case. Let me explain to you why we feel so strongly that this establishment of a non-driver driver's licence is so important to us. For many, many years the blind, deaf-blind and partially sighted in Ontario have not had an acceptable means of identifying who they are. There are many services that many people take for granted, such as opening a bank account, cashing a cheque, going to rent a video, renting a tuxedo and numerous, numerous cases where people try to access everyday services and they are denied access to these services because they do not possess a driver's licence. Unfortunately, with my guide dog, I'm not allowed to drive. It would be interesting if I did try, but I digress. Implementing Bill 85, although I realize our initiative is only a small part of the enhanced driver's licence, would satisfy the need of giving us the access to all the services I mentioned.

The other thing I should point out is that the main mandate of the Ontarians with Disabilities Act, which was passed in 2005, is to eliminate barriers. It is our opinion that implementing this bill will do just that. It will allow us access to cash cheques in the bank, open bank accounts and do all those things I mentioned. Even last week, I should tell you, with the elections that took place, even with a passport, people were still denied access to vote, because a passport alone was not sufficient. Yes, it has your picture, signature, date of birth and name, but it does not include your address. The enhanced driver's licence, we believe, does and would cover that.

The other thing I wish to point out is that not only would blind, deaf-blind and partially sighted people be well served by this but also all other non-drivers in Ontario, including seniors, students going to school and other non-drivers. With the costs of maintaining a vehicle, maintaining its upkeep and paying for insurance spiralling, many people simply choose not to drive because it is too expensive for them, so they are in the same position as we are: not having a valid piece of identification to identify to people and validate who they are.

In conclusion, the only thing I can say is implementing Bill 85 would eliminate the barriers we encounter and would provide additional revenue to the government from people who currently don't have a driver's licence and would help economically in these tough times. I hope that the committee will recommend this bill be passed and implemented. I thank you again for allowing me to speak.

The Vice-Chair (Mr. David Orazietti): Thank you very much, Mr. Wiseman, for your presentation, and if you can bear with us, we have questions for a few minutes. Each caucus will have two minutes. We'll start with Mr. Klees.

Mr. Frank Klees: Thank you, Mr. Wiseman, for your presentation and for a very unique perspective on this issue. Is there some information specifically that would apply to blind, deaf-blind or partially blind individuals that you would want to see on this information to meet your specific needs?

Mr. Phil Wiseman: Well, to be very honest with you, when this idea was first brought to our attention, to show you how simple it was back then, it was the same plastic photo ID of a driver's licence that on the back had a sticker indicating "For identification purposes only." Personally, I don't think we're after anything specific that isn't already on a driver's licence.

Perhaps the only thing I could add is that there could be some tactile marking on the identification card for anyone who can read Braille, or something that would be unique. It could be a notch at the corner of the card to help them identify that this is my driver's licence. People

who are generally blind have unique ways of being able to identify which card is which. For sure, if it has Braille on it, that would be best.

I realize on a small card you can't put large print, but that's why I say in terms of information on it, I cannot see anything in addition that we would be asking for. We just want a card for ID.

1710

Mr. Frank Klees: That's why I asked this specific question, because we need that perspective. I know the parliamentary assistant is listening and the government will take that into consideration. Thank you so much.

Mr. Phil Wiseman: Thank you very much.

The Vice-Chair (Mr. David Orazietti): Mr. Bisson.

Mr. Gilles Bisson: Thank you very much. Your suggestion that we put Braille on the card is one that we will take seriously. We'll put an amendment forward on behalf of yourself and others. That's something that we should have, quite frankly, thought about at this point; I'm surprised we didn't. But such is the struggle.

In regard to this, I understand the need for having some sort of photo ID for the everyday life interactions that we have in society. I think all of us have supported that on all sides of the House. However, do you have any concerns about the data being collected being data that might not be suitable for privacy issues?

Mr. Phil Wiseman: Well, I suppose the only thing that we can ask for is that the information on the card be as secure as possible. I'm not a technical person, so I'm hardly in a position to suggest how that be done. But in the worst-case scenario, there is no such technology out there that would keep it secure. We would be just as happy if we could have the plasticized driver's photo ID with a sticker on the back. That would still meet our needs. I know that's very simplistic, but we figure as long as you're enhancing the driver's licence, we are pleased that our needs are being met with this bill.

The Vice-Chair (Mr. David Orazietti): Mr. Brown.

Mr. Michael A. Brown: Thank you, Mr. Wiseman. I appreciate your comments. Just to be clear—there seems to be some confusion. There are actually four cards being proposed here. There's a photo ID card, a driver's licence, an enhanced photo ID card, which could be used for crossing borders, and an enhanced driver's licence. I was just mentioning that to be helpful. The information on the normal photo ID card would be treated the same way as the driver's licence.

I think my colleague has a question.

Mr. Phil Wiseman: Okay. Thank you.

Mrs. Carol Mitchell: Thank you, Mr. Wiseman. I just have a quick question.

The Vice-Chair (Mr. David Orazietti): One minute, Mr. Wiseman—if you have time for one more question.

Mr. Phil Wiseman: I'm sorry.

Mrs. Carol Mitchell: I just wanted to give you the opportunity, Mr. Wiseman. In your conclusion, you've stated that you have some concerns regarding privacy. I just wanted to give you the opportunity to expand on what your concerns are directly. I know they're included with your brief.

Mr. Phil Wiseman: I'm sorry, could you please repeat the question? My hearing aid has died on me, so I'm a little bit hard of hearing.

Mrs. Carol Mitchell: In your conclusion of your paper that you were presenting today, you have said that you have concerns regarding privacy that you want to see addressed, and you talked about your mandate. I wanted to give you the opportunity to specifically address what your top concerns are with regard to privacy.

Mr. Phil Wiseman: I assume that when I say "privacy," you're prepared to guard against any hackers who could tap into the database. I assume with the information being maintained on a database that stores all of this information, we would want to ensure that this information be kept secure and confidential—encrypted, I assume. I can't think of anything else that we would be asking for to ensure that the information remains secure, safe and private. I'm sorry, that's about all I can say.

Mrs. Carol Mitchell: Thank you very much.

The Vice-Chair (Mr. David Orazietti): Thank you, Mr. Wiseman, for your presentation.

Committee, just before we wrap up, a couple of items regarding the subcommittee report: that the research office will provide the committee with a summary of the presentations prior to noon on Wednesday this week, October 22; that for administrative purposes, the proposed amendments will be filed with the committee clerk by 5 p.m. on Thursday, October 23; and that for our meeting purposes, clause-by-clause will be next week, a week today, on October 27, in committee room 151.

That concludes today's presentations.

The committee adjourned at 1715.

CONTENTS

Monday 20 October 2008