HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 076 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, October 5, 2017

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, October 5, 2017

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Let's commence the meeting. It's 8:45, and we want to respect everyone's time.

Notwithstanding all the noise to the contrary coming from the Liberal side, I'm going to get the 76th meeting of the Standing Committee on Public Safety and National Security started.

We have two witnesses in the first hour. We have Brenda McPhail of the the Canadian Civil Liberties Association. As an individual, we have Eric Jacksch.

Given the temerity of technology, I'm going to ask Ms. McPhail to speak first in anticipation that we might have some sort of technological failure. Then, colleagues, I'm going to reserve five minutes at the end of the meeting to go in camera to receive the subcommittee's report.

The floor is yours, Ms. McPhail.

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association): Thank you to the committee for allowing the Canadian Civil Liberties Association the opportunity to appear before you today and speak on Bill C-21.

I'm going to focus on three topics: first, the need to for appropriate frameworks including explicit privacy protection for information sharing that happens between the CBP and the CBSA; second, the need to ensure that critical details about how the collection of this information will take place receives public attention and parliamentary debate rather than relying excessively on regulations; and third, the need to increase CBSA accountability commensurately with this significant increase in their powers.

The information that Canada will collect and share with the United States after Bill C-21 is passed includes biographical information as well as the date, time, and place of entry or exit for every traveller crossing the Canadian border, including Canadian citizens.

This is information on literally millions of Canadians. StatsCan suggests that in January 2017 alone Canadians made 3.6 million trips to the U.S. It also allows for information about every person who boards a plane, train, bus, or ship—if those conveyances are prescribed, because that prescription is left to regulation—in Canada to be collected and shared.

When the beyond the border agreement was signed, CCLA along with the ACLU in the United States and Privacy International in the U.K. developed and released a series of core legal principles for sharing the U.S.-Canada security perimeter. In respect of information sharing, we recommended that it should be restricted to the particular purpose—not used, disseminated, or stored for secondary uses. It needs to be subject to rules limiting the duration of retention to reasonable periods, and it should be subject to independent oversight review and accountability procedures. In particular, when the laws of the two countries differ, the highest standard that grants the best protections to individuals should prevail.

As an example of the problems introduced by different privacy standards, we're concerned that at the time this bill was originally discussed in 2014 one source suggested that Canada had decided to limit the time they could retain personally identifiable information to 15 years. The U.S. has said they reserve the right to retain it for 75 years or longer. Even 15 years is a long time, and it's worth considering whether or not that's the right time frame. It is highly questionable that Canada could maintain control over the uses of information through a memorandum of agreement with the U.S. for as long as a lifetime .

We believe the responsibility for taking such principles seriously should be explicit in the legislation. In addition to the current amendments to Bill C-21, we would suggest including an amendment to add a preamble similar to that found in the recent national security legislation, Bill C-59, and similar to that found in section 3 of the Immigration and Refugee Protection Act, which is another act that CBSA administers. Both of these pieces of legislation explicitly identify the responsibility of customs enforcement officers to carry out their responsibilities in a manner that safeguards the rights and freedoms of Canadians and that respects the Charter of Rights and Freedoms. One might argue that it's incumbent on them to do so whether or not that clause is inserted in the legislation, but we would argue that there is both practical and symbolic value in including it in the Customs Act at this time.

On a pragmatic level, one way to ensure that privacy protections are in place is to conduct privacy impact assessments. Clearly, for a project of this scope, which is going to collect information on millions of Canadians, these assessments should be undertaken before information is collected under this legislation and ideally in time to inform the regulations. The assessments should be reviewed by the Privacy Commissioner of Canada, and an executive summary should be publicly reported.

We realize that Bill C-21 is enabling legislation and will continue a process that has already begun. In fact, there were privacy impact assessments for the pilot stages of this project before Canadian information was collected, but these assessments need to be updated in light of the expanded collection.

CBSA also committed to conducting an analysis on all uses of personal information by all parties involved in the sharing of biographic entry data, and while that analysis to my knowledge is not publicly available, I would suggest that, as an important precautionary step before expanding the scope, the committee might wish to see if that analysis actually took place, and figure out how it's working now before we expand it.

● (0850)

I'd also just like to flag that in 2015, in his spring report, the Auditor General expressed concerns that the CBSA's project management framework was not conducting risk assessments at appropriate times. That would be another area where the committee might want to make sure the technological infrastructures as well as the policy infrastructures around this information are appropriately secure.

In relation to regulations, clause 2 of Bill C-21 amends the act so that proposed subsection 92(1) will allow the CBSA to collect information from prescribed sources in the prescribed circumstances, within the prescribed time, and in the prescribed manner, and then allow the Governor in Council to make regulations to fill in those blanks. The problem is that leaving so much to be prescribed means a process that is less public, less transparent, and less accountable.

In simpler terms, who we are going to collect the information from, why, when, and how is not clearly specified anywhere in the legislation, but these aren't inconsequential details. Knowing them would allow us to evaluate the nature of the collection process, weigh the potential risks to privacy, and better understand the potential costs of a leak or breach. Knowing the source of information allows us to judge its integrity. Knowing why and how it can be collected allows us to assess the proportionality of the collection in relation to its purpose. Clichés sometimes ring true: the devil is in the details.

While we appreciate the need to keep the legislation technologically neutral and flexible, flexible should not mean completely open-ended, particularly because regulations can be changed quietly, largely out of public view, with a much less democratic process than the one we're engaging in today. What current drafters intend to include in the regulations may not be what subsequent governments would choose.

We are, at this time, witness to a dramatic change in policy direction in one of our neighbours. We should take that lesson to heart. When we're talking about practices that engage charter-protected rights to privacy and mobility, safeguards should be enshrined in law. To this end we recommend the committee consider what aspects of the collection process could and should reasonably be included in the legislation.

Lastly, this bill expands CBSA powers but does not increase accountability. CBSA is still the only federal agency with security and law enforcement powers that doesn't have comprehensive, independent oversight or review of its actions. We argue that it's unwise to continue expanding their powers without increasing that accountability framework.

CBSA will now be allowed to share information for the purposes of enforcing the Employment Insurance Act and the Old Age Security Act. If mistakes are made, that could have highly detrimental effects on individuals. There should be a possibility for individuals to appeal the accuracy of the information to an independent body.

CBSA's role in controlling the exit of goods and people from Canada is expanding. The bill creates a new requirement for people exiting Canada now to answer the questions of a CBSA officer truthfully. Answering falsely is an offence. This is a broad power. There is no question that people should have to respond truthfully to a CBSA officer, but I'm sure we've all seen recent stories about agents on both sides of the border asking questions that people are alleging relate to racial background, religious beliefs, and political opinions. Potentially allowing some form of this intrusive and problematic questioning on exit as well as entry doubles the opportunity for potential abuses of power.

While creating an independent review body for the CBSA is clearly beyond the scope of this bill, allowing a potential escalation of a non-problem while simultaneously failing to provide a recourse to an independent civilian body to receive complaints, review policies or officer conduct, or investigate potential misconduct is simply wrong. Every time the CBSA's powers are increased, the lack of an independent review body to provide additional and necessary safeguards becomes more problematic.

Thank you for the opportunity to provide these comments. I look forward to your questions.

● (0855)

The Chair: Thank you, Ms. McPhail. Thank you for staying within the time limit.

Mr. Jacksch.

Mr. Eric Jacksch (As an Individual): Good morning, Mr. Chairman and members of the committee. My name is Eric Jacksch, and I'm pleased to be here to discuss Bill C-21.

By way of background, I have a B.A. in sociology-criminology and started my career working as a correctional officer and probation and parole officer for the Province of Ontario. I've also had the great privilege of serving in the Canadian Forces Reserve, both the infantry and intelligence branches. My interest in high-tech, combined with a part-time software development business, drew me to Ottawa during the tech boom in the mid-nineties, and I quickly specialized in what we now call cybersecurity.

I have more than 20 years experience in information security, as well as a background in physical security. I am board-certified in security management by ASIS International, and hold their certified protection professional, or CPP designation. I also hold the certified information security manager designation from ISACA, previously known as the Information Systems Audit and Control Association, and the certified information systems security professional or CISSP designation from the international information system security certification consortium, also known as $(ISC)^2$.

So far in my career, I've had the pleasure of providing security services to a variety of federal, provincial, and municipal governments, as well as some of the world's largest banks, automakers, insurance companies, and postal organizations. Consulting engagements have taken me across Canada and the United States, and to the U.K., Switzerland, Spain, Netherlands, Japan, and Singapore. I have taught courses, spoken at conferences, and written numerous articles.

Perhaps most relevant to these proceedings, I have performed risk and privacy assessments for Canadian federal government departments, as well as provincial and private sector organizations required to meet Government of Canada security requirements.

A significant challenge in cybersecurity is education and awareness. In addition to running securityshelf.com, a security news aggregation site, I write a column for IT in Canada. That first put the issues underlying Bill C-21 on my radar.

Back in March 2016, just after Prime Minister Trudeau's visit to Washington, I read articles in the media suggesting that Canada was gearing up to start sharing more personal information with the United States. I thought it would make an interesting article for my column, so I did some research.

As it turned out, the media coverage was mostly hype. However, it did make for an interesting article entitled, “No, the sky is not falling”. You're welcome to visit canadait.com to read that and more of my articles.

I'm sure you've all been briefed on the history, but in summary, as I understand it, in December 2011, then prime minister Steven Harper and president Barack Obama released the beyond the border action plan for perimeter security and economic competitiveness. As part of the plan, Canada and the United States committed to establishing a coordinated entry and exit information system that includes sharing information so that the record of a land entry into one country can be used to establish an exit record from the other.

According to the CBSA, phase one ran from September 2012 to January 2013, during which time:

> ...both countries tested their capacity to exchange and reconcile biographic entry information of third-country nationals (non-U.S. or Canadian citizens), permanent residents of Canada who are not U.S. citizens and lawful permanent residents of the U.S. who are not Canadian citizens [having crossed] at four land ports of entry in British Columbia/Washington State and Ontario/New York.

In June 2013, phase two expanded the program to cover all common land border ports of entry with the processing capacity to capture traveller passage as an electronic record. During this phase, information was not shared “on Canadian [or U.S.] citizens, Registered Indians, or protected persons.”

What we are essentially talking about today is the next phase of the entry-exit initiative, and expanding information sharing to all travellers at land border crossings. It's understandable that Canadians are concerned about the prospect of Canada and the United States sharing personal information. From a security perspective, I see three areas of potential concern.

First, there's the actual implementation of information sharing between CBSA and U.S. Customs and Border Protection. To understand that impact, we need to consider what's being shared. I'll quote the privacy impact assessment summary for phase two, published by the CBSA:

● (0900)

> At entry, each country presently collects the following data elements as agreed to for the Phase II exchange: Name (first, middle, last), Date of Birth, Nationality/ Citizenship, Gender, Document information (type, number and country of issuance); these elements were demonstrated to be effective in reconciling entry and exit information in Phase I. The only data to be exchanged, which are not already known to the receiving country, will be the date of entry, time of entry and the port through which the individual has entered.

Assuming that information sharing is constrained to this set of biographical data, which I also see reflected in Bill C-21., the exchange of information between CBSA and the U.S. CBP has no practical impact on honest, law-abiding travellers.

The second area is how this information is protected in transit and rest. Canada has proven methodologies to assess cybersecurity risk, and specific guidance on the security controls required to effectively protect this type of information is readily available. Assuming that the cybersecurity aspects of this data sharing are taken seriously, there is minimal risk to Canadians.

The third and perhaps most difficult area is ensuring that information is used only for the intended purposes. When any entity, public or private, has information, there's always a temptation to find new uses for it. Abuse of information by individuals is a problem. Informal information sharing between organizations can give rise to serious security and privacy concerns.

I understand that the Privacy Commissioner has already been involved, and I hope that continues. I also applaud CBSA for publishing a summary of their privacy impact assessment online. As legislators, I urge you to ensure that appropriate privacy controls are in place and to make it clear to Canadians how and under what circumstances this entry and exit information may be shared outside of CBSA.

Section 6 of the charter guarantees every citizen the right to enter, remain in, and leave Canada, but it doesn't say that they can do so anonymously. Canada already tracks entry and exit information for air travellers, and from a security perspective, expanding it to land border crossings makes good sense. I don't foresee any significant security obstacles in the proposed approach.

Thank you for the opportunity to speak on this topic. I welcome your questions.

The Chair: Thank you, Mr. Jacksch.

Our first questioner, for seven minutes, is Madam Damoff.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you very much.

Thank you to both witnesses for being here today.

To Ms. McPhail of the Canadian Civil Liberties Association, have you had an opportunity to read the CBSA's privacy impact assessment? You mentioned that they should do one, and I've looked at the one they have done. Have you read the one that has been done?

Ms. Brenda McPhail: I've read the executive summary available on the website, which is the only version available to the public.

Ms. Pam Damoff: Okay. Maybe I misunderstood you. I thought you said that they should do a privacy impact assessment on the bill.

Ms. Brenda McPhail: This is a process that has already begun, the process of collecting exit and entry data. As my fellow presenter mentioned, there was a phase one and a phase two, during which information was collected, just not from Canadian citizens or U.S. citizens. It was collected from third-party nationals and other groups of people. At that time, impact assessments were done for that collection.

My argument is that, while they're expanding the scope of the information collection, they should be looking to make sure that there are no additional privacy risks to Canadian information. I would note that in their assessment plan, they actually indicate that they intend to conduct such an assessment for phase three. They acknowledge that this is a large expansion of the information that's going to be collected, so I would just recommend that we ensure that they actually follow through on that.

● (0905)

Ms. Pam Damoff: Thank you for clarifying that.

As you just mentioned, it is being done now, but not for Canadian citizens. Certainly, we've heard testimony, and there have been articles written about how this will assist law enforcement for things like amber alerts, child sex offenders, and human traffickers. There are certainly benefits in terms of law enforcement, in particular for amber alerts, to make sure that we don't have children being taken out of the country.

I get the impression that you're generally okay with this bill. You just have concerns with aspects of it. Is that correct?

Ms. Brenda McPhail: Yes. That's correct.

Ms. Pam Damoff: Okay.

You gave us some recommendations, and I always appreciate it when witnesses provide us with recommendations on how we can improve legislation. Have you looked at the legislation on entry and exit in other countries, to see if there are any best practices elsewhere that you could share with us? We're one of the few countries that doesn't have this requirement at the present time.

I might put that to both witnesses, actually.

Ms. Brenda McPhail: I'm sorry. I haven't done that sort of cross-cultural, cross-country comparison.

Ms. Pam Damoff: That's fine.

Mr. Jacksch, have you done any at all?

Mr. Eric Jacksch: No. I haven't.

Ms. Pam Damoff: All right.

Thank you.

One of the things that was brought up had to do with storage and retention. You brought that up, Ms. McPhail, in terms of the timing, and you thought it was too long. Do you have recommended timing that you think would be appropriate?

Ms. Brenda McPhail: My understanding is that the 15-year time frame was negotiated with the Privacy Commissioner of Canada in one of the earlier phases of this. From our perspective, the shortest reasonable time to keep information is always the best. If the 15-year time frame is what has been agreed upon with the Privacy Commissioner, then I think that's fine. We would hate to see it go any longer than that, and we would really like to see the retention periods rationalized between the two countries, because the difference between 15 and 75 years is a lot.

Ms. Pam Damoff: Do you have any comments on that?

Mr. Eric Jacksch: I would echo the same general comment, that information really should only be retained for the period of time it's required. It's a little difficult to understand why entry and exit data would have any value 50 or 75 years after the event.

One example I like to use is CBSA. Most organizations are required to maintain tax records for seven or eight years, and beyond that even the financial aspects of individuals and companies are primarily considered irrelevant.

Certainly that's a good topic for negotiation with the Privacy Commissioner, and I'd like to see it reasonably short, also realizing there's a cost to maintaining that information.

Ms. Pam Damoff: I should also mention that we can set our time frame and discuss with the Americans, but obviously we have no control over what they decide to do. If they have determined 75 years, we can have those conversations but we obviously can't make any requirements towards the U.S. to shorten that time frame.

Ms. McPhail, you were talking about oversight of CBSA. I would just mention, though, that it is included in Bill C-59. While it doesn't exist right now, it is something that is included in the legislation that is before the House. We anticipate and hope to see that legislation at this committee, and then of course go through the Senate. That is something that will be taking place once that legislation becomes finalized, and we'll fill the gap that currently exists. I recognize this came here first, but we are looking at doing that. You were aware of that, I'm assuming.

Ms. Brenda McPhail: Yes. My understanding is that under the terms of Bill C-59 it is the national security functions of CBSA that will be brought under the aegis of the new integrated review committee. It's not clear to me whether or not the more specifically customs-related activities of CBSA are covered under that. It's actually a bit unclear the extent to which all the activities of CBSA are covered, because the legislation specifies that it will be their national security activities that are subject to review by that committee.

Ms. Pam Damoff: That's a question we can ask when we get that bill.

Thank you very much for your time.

● (0910)

The Chair: Thank you, Ms. Damoff.

Mr. MacKenzie.

Mr. Dave MacKenzie (Oxford, CPC): Thank you, Mr. Chair, and thank you to the witnesses for being here.

This bill comes out of an agreement from a few years ago. One of the things that we always hear is the concern about sharing the information with the Americans. In fact, most of the information the Americans would have on us in this regard is when Canadians go into the United States. We don't have any perfect rights in our system where we can go into the United States without identifying ourselves, so they collect that information as it is when we go into the United States. What would our concerns be, beyond the fact that the Americans have already collected the information and they share it back with the Canadian authorities?

Maybe you can start, Mr. Jacksch.

Mr. Eric Jacksch: I think those concerns are very minimal. When a Canadian or anyone in Canada enters the U.S. at a land border crossing, it's in fact that individual who's providing his or her personal information to the Government of the United States and essentially agreeing to the laws of the United States with respect to the use and storage of that information. It's really difficult to envision how the fact that the United States then sends a record back to Canada saying this person has just left Canada would impact an honest, law-abiding traveller.

Mr. Dave MacKenzie: Ms. McPhail, do you have any comments?

Ms. Brenda McPhail: I would agree. I think there's relatively minimal impact. Our concerns are around making sure that the system designed to store and retain this information is secure, to the extent that it's needed, and that privacy protections are in place.

One of the concerns with collecting information—my fellow presenter mentioned it—is around function creep. Something that's not mentioned in this bill is biometric information. In particular, if this is something that would later lay a foundation for the collection of that information to be added to this, it's really important that the infrastructures be secure.

Mr. Dave MacKenzie: If we go to that, there would be further discussions with respect to biometrics being collected, and I think that's the time that we'd need—

Ms. Brenda McPhail: Yes, absolutely.

Mr. Dave MacKenzie: At this point, it would seem, for the most part, that it's not intrusive on Canadians' rights. One of the things that all of us frequently hear is that when somebody gets to the American side, there is questioning on the American side of Canadians going in, but that has nothing to do with the collection of this information. Would both of you agree with that?

Mr. Eric Jacksch: Yes.

Mr. Dave MacKenzie: Once we've collected the information—and we've already been told that there will be some sharing with other government agencies with respect to government benefit programs and so on—what does that raise with respect to your concerns on privacy?

Ms. Brenda McPhail: I think, whatever information is being shared, it's incumbent on us to make sure it's accurate and that there's a way for people to challenge the accuracy. It might be appropriate—and this is outside the scope of the bill—to think about whether or not the regulations.... If people are going to be penalized for leaving the country, we should make sure that regulations are in place and that the rules around when you're allowed to leave and when you can come back are reasonable in relation to old age security and unemployment. Again, that's outside the scope of this bill.

Mr. Dave MacKenzie: Sure.

Mr. Eric Jacksch: I think the key is transparency, so that Canadians know what the rules are, that they know how and under what circumstances that information can be shared outside of CBSA, and that there are safeguards to ensure that it doesn't mushroom into something that Parliament didn't intend.

Mr. Dave MacKenzie: Would you agree that someone who feels information has been shared with another government agency that has brought them into question with respect to receiving benefits to which they may or may not have been entitled have that appeal process within the organization that's providing the benefits? I don't know that CBSA would necessarily be part of the equation there. If it's your documentation that's forwarded back, I guess the only issue would be whether it was accurate information to begin with.

Mr. Eric Jacksch: There are several fundamental privacy principles, and one of them is the ability to challenge information that's incorrect. In this situation, what it comes down to is where that information is held and where should that challenge occur. Would it occur at CBSA, or would it occur with one of the other agencies that it may be shared with?

● (0915)

Mr. Dave MacKenzie: But they're all appealable to those agencies.

Mr. Eric Jacksch: I would hope so.

Mr. Dave MacKenzie: Okay.

What weaknesses do you see in the system? We'll start with Mr. Jacksch.

Mr. Eric Jacksch: I don't see any. As I mentioned in my opening statement, I think that the third area of concern, ensuring that there isn't an unintended expansion in the use of that information, is critical. That would be my primary concern, and I suggest that the committee carefully consider if it would be appropriate to put some additional restrictions on that use. We have other government departments with similar approaches, and that may be helpful.

Mr. Dave MacKenzie: Mr. Chair, I'm wondering if Ms. McPhail could answer the same question.

Ms. Brenda McPhail: In terms of weaknesses of the systems for information collection and storage, I'm not sure that we can see what those weaknesses are. The committee, frankly, would be in a better position to interrogate those systems.

In terms of weaknesses in the way that the framing around the collection of this information is done, I'd just go back to my point that basically every detail about the information that's going to be collected is left to be prescribed in regulations. We might want to consider whether that's entirely appropriate or whether some of those details should be included in the legislation just so it's really clear what we're collecting, how it can be collected, and from whom. How do we ensure the integrity of that information if we can't interrogate those facts?

Mr. Dave MacKenzie: Thank you very much, Ms. McPhail.

The Chair: Thank you, Mr. MacKenzie.

[*Translation*]

Mr. Dubé, you have the floor for seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

[*English*]

Ms. McPhail, when it comes to information sharing, I think I understood the minister's answer correctly when I asked him this question on Tuesday, but is one of the concerns the fact that, with what was formerly Bill C-51, we already have the information sharing regime in place between government agencies, so this information being collected can be shared pretty broadly throughout different agencies that don't necessarily have the same accountability mechanisms in place as, for example, some of the national security agencies might have?

Ms. Brenda McPhail: Yes. I think that is the case. It's possible that the revisions under Bill C-59 will ever so slightly limit some of those concerns in relation to stricter proportionality requirements around sharing.

Still, once information is shared under that agreement, we don't know how far it can go, and again that brings up the concerns about whether the uses of that information will be limited to what it was collected for.

Mr. Matthew Dubé: Thank you.

I want to clarify some aspects. You mentioned the importance of redress and being able to refer to an independent body in the event of mistaken identity or erroneous information. Hopefully I'm not misstating what was expressed, but when I asked CBSA the question about what type of redress system would be in place, they essentially seemed to imply that the person would have to deal with whatever government agency was in question.

For example, if you were looking at a situation with regard to old age security and you felt that somehow some issue was brought up about when you actually left the country, you would have to deal with the ministry responsible for administering OAS as opposed to having any proper recourse with regard to CBSA.

Do you feel that this is accurate, and if so, do you think we can amend the bill or bring in even larger changes beyond the scope of this to make sure that CBSA remains accountable for the accuracy of that information?

Ms. Brenda McPhail: It would be entirely appropriate to include a provision that, when collecting and sharing information that can have such very significant effects on individual Canadians, CBSA be responsible for accuracy. There should be some process for interrogating the accuracy of that information in an appeals process, and the onus to certify that accuracy should be on CBSA and not individuals or other organizations that are not responsible for collecting it or maintaining it.

Mr. Matthew Dubé: Okay. Thank you.

We talked about the risk of profiling. It's an interesting piece, because one of the things that seems to be emphasized here is to not be worried because it's only page 2 of the passport. When we look at things such as the country issuing the document of citizenship or nationality, and when we see how people who are Canadian citizens have been treated at the border, is there any concern that despite the fact that the information is very specific and limited, there's nonetheless enough in there for someone to infer things that might not be the case, especially when one of the stated intentions of the bill is to go after people who might radicalize or supposedly radicalized individuals who might be leaving the country for nefarious reasons?

● (0920)

Ms. Brenda McPhail: Absolutely. We know people infer things from country of origin all the time. It's a common problem. We know there has been, as I have mentioned, an increase in intrusive questioning, including questions specifically targeted at people with particular backgrounds, from Middle Eastern countries, people who practise the Muslim faith in particular, and there is enough information on that page 2 to permit at least the beginning of that kind of profiling.

The reality is also that, at the border, whether this is the only information that is shared, it is certainly not the only information that officers will have access to at the time of questioning. Because we're expanding their ability to question at the point of exit as well as the point of entry, we are increasing the risk that intrusive questioning is going to happen and that is going to be difficult. I'll leave it at that.

Mr. Matthew Dubé: Okay. Thank you.

I have a question for both of you with regard to some of the concerns about how long the information is held for and things like that. There has been a change, in particular, through one of the recent executive orders that essentially removed legal privacy protections from non-U.S. citizens in the U.S. With this type of trend, if I can put it that way, is there a concern with the information being shared potentially between the two agencies about not only the length of time but the actual protections that are put in place and where that information might end up?

We could even dare say this would be outside of government agencies and even within the private sector. In particular, we've heard that even with the NAFTA renegotiations one of the American asks has been a broader ability to share information and things like that, which aren't necessarily theirs, and omit them from certain legal protections.

Could I hear both of you on that, please?

Mr. Eric Jacksch: As Canadians, we don't get to dictate U.S. policy, so when Canadians appear or anyone appears at a U.S. border, they have to accept U.S. law. Certainly my advice to the U.S. government would be the same as I've given this committee, which is you collect information, you use it for the purpose for which it was collected, and when it's no longer necessary or relevant, you safely dispose of that information.

In terms of the impact on Canadians, I think it's important to realize that the data flow from Canada to the United States is occurring as people have already left the United States. While I share the concerns on issues such as profiling, the reality is the trigger for Canada to send this record to the United States is someone leaving the United States and entering Canada and not the other way around, so it's difficult to understand how that, again, would have a significant impact on a traveller. I've just left the United States and come to Canada and now Canada is sending the information that the U.S. presumably already has, other than the fact that I've left.

Again, in terms of information retention, it's difficult to know what the United States will do with that, but again the only information that Canada is really giving them that they don't already have is the date, time, and port of exit. If anything as a Canadian, I'd prefer that the United States knows that I left. That way, the next time I show up requesting entry into their country, they're going to have that record and know that when I said I was staying for a week, I stayed for a week.

The Chair: Thank you, Mr. Jacksch and Mr. Dubé.

Mr. Spengemann is next, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Mr. Chair, thank you very much. Ms. McPhail and Mr. Jacksch, thank you both for being here for your expertise.

Ms. McPhail, I wanted to start with you with a question just to follow up on an earlier comment with respect to the scope of what's being collected. Is it correct that it's your testimony that outside of the current dataset that was enumerated for the committee, other things could in the future be collected without an amendment to the legislation?

The committee received testimony in an earlier session that for any additional data points to be collected, the legislation would again have to be amended. I just wanted to, for the record, clarify your views on that.

Ms. Brenda McPhail: I believe that's true. I believe that what's left to be prescribed in regulations is not what kinds of information can be collected, but from where and from whom and then how. It is my understanding that you would have to amend the legislation for different kinds of information.

● (0925)

Mr. Sven Spengemann: That's helpful. Thanks very much.

You mentioned earlier in your comments that one of the things that we should look at before going forward with new legislation is to see how things are working now. I wanted to take the opportunity of your presence here to ask you if you could outline from your experience looking backward—and not necessarily at the specific issue but at privacy more broadly—the differences and also the convergence between Canadian and American privacy approaches and cultures.

Are there fundamental differences in the way Americans look at data collection and privacy that would give cause for concern in the way this legislation is framed?

Ms. Brenda McPhail: Canadians and Americans have always had somewhat different privacy cultures. Under the current administration, the current trend has been to diminish privacy protections, particularly for foreign nationals, and Canadians, of course, are foreign nationals in the U.S. What this does is it makes it more incumbent on us....

As my colleague pointed out, we don't get to dictate American policy, but what we do get to do with individual agreements is negotiate our terms. As general privacy protections in the U.S. are under siege and being eroded in a range of ways, it makes it all the more important that in specific agreements we make sure that our Canadian values are addressed in relation to agreements, because when there is no general protection, the terms of the individual agreement is all we have to make sure that we're safe.

Mr. Sven Spengemann: Thank you for that.

Does the Canadian Civil Liberties Association keep any data on public opinion? Do you do any polling? Do you review any primary data on how the Canadian public feels about privacy issues?

Ms. Brenda McPhail: We don't do any formal polling. What we do have is a fairly extensive public inquiries program where people call in to us with their civil liberties concerns. Over the last eight months, the number of people calling in with concerns about privacy issues at the border has tripled, which for a small organization is a significant increase.

Mr. Sven Spengemann: For the benefit of the committee and the Canadian public, could you speak about the differences between public and commercial privacy concerns? The Canadian public is travelling extensively. We share our flight agenda to collect air miles or Aeroplan points. We share our travel reservations to collect hotel reward points, and anything up to and including gasoline purchases are basically shared through rewards points systems, which are made available to all sorts of vendors contractually.

How does that compare with how Canadians feel and what Canadian expectations are with respect to publicly collected data? Are they two different worlds? There's a propensity for Canadians to share their data through commercial channels, or even through social media like Facebook or Instagram. Do we do that differently with respect to considerations related to public agencies?

Ms. Brenda McPhail: There is a fundamental difference between Canadians as consumers making an informed choice to share data in exchange for a perceived benefit or convenience, and the state mandating that information they have to give to the state can be shared with other parties with relatively little control by individuals. It's a bit of a different thing.

There's also an increasingly blurred boundary between public and private. We know that the state is interested in using information that's publicly available but not necessarily shared for the purposes that individuals would have expected it to be used by the state. This is something we're concerned about in a more general way.

Mr. Sven Spengemann: Would you be in a position to comment on whether Canadian public opinion has been shaped more by the commercial environment or the public environment? Or is it really a bifurcation of opinion when it comes to the difference between the commercial travel points scenario and publicly held information on health, immigration, or travel?

Ms. Brenda McPhail: What we're increasingly seeing—and polling by the Privacy Commissioner of Canada supports this—is that people feel as though they're losing control of their information across all sectors, and in all ways. They're losing control of what the public sector does with it, they're losing control of what the private sector is doing with it, and they're not happy about it. I think there's a real blurring of boundaries. I think people are unhappy in both regards, and I'm not sure that everyone necessarily makes the distinction. They're just feeling that all of their information is going out and they don't know what's going to happen to it.

● (0930)

Mr. Sven Spengemann: I think it's clause 2 of the legislation that creates the authority for CBSA and public officials to collect data. It's framed in a permissive way—the legislation says that XYZ official may collect information. We had testimony from the regulators themselves who said this is the way it's typically done in the Department of Justice. The permissive environment is created, and then through regulation precision is restored regarding how the information is collected.

Would you say that this discretionary authority gives rise to concerns that an officer may or may not decide to collect the data, or would the officer be ultimately so confined by regulation that there is very little discretion?

Ms. Brenda McPhail: Less permissive is better than more permissive in our opinion. Things that you mean to have enshrined in legislation should be there.

Mr. Sven Spengemann: Thank you.

The Chair: Now that was an instruction in brevity.

Ms. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chairman.

We need only look at some of the terrorist attacks that have occurred in Europe—where it has taken days for authorities to track down perpetrators to make sure they're not on the way to conducting another attack—to understand why the entry-exit data is important for security purposes.

I understand that part of the reason for the delay behind the implementation of the full beyond the border plan is the decision to expand the sharing of travellers' entry and exit information with other Canadian federal departments. One of those is the Canada Revenue Agency.

Can you explain how the travel exit-entry data would be relevant and worthwhile to the Canada Revenue Agency in terms of protecting citizens, or preventing fraud or anything else?

Ms. Brenda McPhail: I'm not sure. I share your question in relation to that.

I would note that under the Security of Canada Information Sharing Act, information sharing was vastly expanded, and the scope of agencies that were identified as having potentially something to do with national security was extremely broad. That's something we criticized in relation to Bill C-51, and it seems reasonable to continue to criticize it here.

Mrs. Cheryl Gallant: Other than a cross-comparison of data, I don't see how they would be gleaning whether or not somebody is cheating on their taxes from this information. It mystifies me as to why they would do this.

For Mr. Jacksch, you say that the sky is not falling, and law-abiding citizens don't have anything to worry about in terms of their information being safeguarded or misused by Canadian or American agencies. However, we see, such as with NATO, that they fend off over 500 cyber-attacks a month. The Pentagon is always fending them off.

Now we don't know about the ones they're not able to fend off. They're kept in-house, of course. Even here at the House of Commons, we will from time to time lose all our connectivity because they've been rendered helpless until they reboot the system and clean out the malware.

Given that not only is it a segregated computer system but that we're living in the Internet of things, how can you be so confident that individuals' information is totally protected?

Mr. Eric Jacksch: I'm not sure I'd use the words “totally protected”, but we can manage those risks. Canada, and particularly the federal government in Canada, has a good process. We have a proven risk assessment methodology. In fact, the Government of Canada process is so good that I often use it with private sector clients.

What it comes down to is the application of what we know. If we correctly architect systems, correctly design systems, perform risk assessments, take seriously the guidance provided for our lead agencies in that space, if we look at, for example, the controls that are suggested by the Communications Security Establishment and ITSG-33, we can build systems that are quite secure and that certainly provide the level of security needed to protect this level of information.

● (0935)

Mrs. Cheryl Gallant: But we had Heartbleed and our science department, NSERC, was attacked.

How can you say with such confidence, given the record of attacks we have had, that this information won't be exposed to a criminal element?

Mr. Eric Jacksch: I'm not saying it won't, but I'm not saying it will either.

Mrs. Cheryl Gallant: Okay.

Mr. Eric Jacksch: All I'm saying is that there are some risks that need to be managed, and I believe the government has the appropriate approaches to secure it.

Mrs. Cheryl Gallant: Thank you.

The Chair: Thank you.

Monsieur Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

Thank you for paying attention to a most sensitive issue that falls under the values of the Canadian Charter of Rights and Freedoms: privacy protection.

You said that you're getting more and more calls and messages with people's fears about their privacy protection. In addition, your organization made its own comments. You said you are concerned about the negative impact of the exchange of information prompted by Bill C-21.

Are those concerns and comments the result of a misunderstanding of Bill C-21? Do you believe that this bill focuses on sharing information that is limited basically to what is on page 2 of the passport and some logistical information? If not, do your concerns simply stem from an analysis based on hypothetical situations and speculations?

[*English*]

Ms. Brenda McPhail: It's important to remember that in the age of big data and data aggregation, small pieces of information that seem inconsequential matter more when they're combined with others. The fact that this information is going to be collected doesn't just mean that someone is only ever going to be looking at the tiny pieces of data that are collected under this bill. This bill is adding to the amount of data that can be collected and aggregated with other information that's known about people.

Knowing, by itself, when someone comes in or leaves can be very useful information in a variety of ways, and it seems harmless, but it's very difficult to predict what any one of the organizations on either side of the border who has access to this information might do with it when it's combined with other things.

It's a hypothetical and general warning. We know that information when combined becomes more powerful.

[*Translation*]

Mr. Michel Picard: Thank you.

Mr. Jacksch,

[*English*]

You come from the intelligence community. I wanted to ask you about the period of time we can hold on to the information. We talked about 15 years. I want your perspective on this period of time, knowing that from the intelligence standpoint, information sometimes becomes useful after a number of years. Therefore, if you limit it too much you may prevent further investigation, not knowing at the time that this information might be useful.

Mr. Eric Jacksch: There is some period of time for which the information is useful. I can't tell you from an intelligence perspective what that time frame is. That would be a good discussion between CBSA, the relevant intelligence agencies, and the Privacy Commissioner, to find that balance of keeping information for an appropriate period of time but not for too long.

Mr. Michel Picard: Do you believe, then, if you want to make sure we protect this information as much as possible, the goal would be to increase the technology, or the human power, the human resources? How do we handle that?

Exchange of information is a transaction of data, but requires technology that is always vulnerable to someone, somewhere.

● (0940)

Mr. Eric Jacksch: I don't have any insight into the mechanics of the current system. I know records are exchanged. I don't know how the systems are designed. I haven't seen any of the risk assessments or been involved in that. Certainly, from a security perspective, the right approach is to ensure that risk assessments are conducted, and that we pay close attention to the guidance that's provided by our lead agencies.

Again, there are a whole host of cybersecurity threats facing individuals and Canada as a whole. Our goal needs to be to manage those threats, and that starts with designing systems with the appropriate controls right from the beginning.

One of the challenges in cybersecurity is that security is often slapped on like a band-aid after the fact. One of the improvements—and I've certainly seen this with some of the government plans I've worked with—is to consider that early in the process. Consider security in the design process, and build in the level of security we need.

Again, I can't speak to the degree to which that's being done with the current system.

Mr. Michel Picard: Thank you, Mr. Chair.

The Chair: I understand my Conservative colleagues don't have a question. In a matter of extreme collegiality, they're going to give the final three minutes to Mr. Fragiskatos.

Mr. Peter Fragiskatos (London North Centre, Lib.): I have to say, Mr. Chair, my very able colleagues have already asked the good questions, so I'm left with a general question here that perhaps cuts to the core of the bill, and security and privacy issues in general terms.

Mr. Jacksch, could you outline for us your view on privacy and security and where governments ought to draw that line?

Mr. Eric Jacksch: Wow, that's a tough one.

The Chair: In three minutes....

Mr. Eric Jacksch: In three minutes, thank you, Mr. Chairman.

There is a balance. Particularly when we're dealing with issues of law enforcement and issues of national security, there is a very delicate balance. I feel for legislators because, on one hand, Canadians demand that you protect them, you protect the country, and you ensure that law enforcement and intelligence agencies are able to do their jobs. On the other hand, Canadians demand privacy.

One of the important elements in that balance is the Privacy Commissioner. I wish I could draw a line and say, “Here is security, here is privacy, and here is where we should sit” but it really depends on the situation and it depends on things like the type of information. I'd urge you to go back to those basic privacy principles. Certainly we've Canadianized them, but the principles in our privacy legislation are drawn from European privacy principles, and they're really principles that are commonly agreed on by many countries around the world. I think those are very helpful to look at.

Mr. Peter Fragiskatos: Thank you very much.

I know and respect the position of the Canadian Civil Liberties Association, Ms. McPhail.

You mentioned something about a preamble in your opening remarks. Could you just touch on that again?

Ms. Brenda McPhail: Yes. In many pieces of recent legislation, there are preambles that specify the general governing principles that should guide the legislation. It's very common to have a preamble that specifically says that the Canadian Charter of Rights and Freedoms should be respected in relation to enforcing the piece of legislation.

It seems that the Customs Act is one of those pieces of legislation currently lacking such a preamble, which would greatly benefit from it. As powers under the Customs Act for search and seizure and questioning increase, it just seems that it would be a worthwhile reminder to say, “Look, all of this has to happen within the framework of our charter and in accordance with the values that we hold as a democratic society”.

Mr. Peter Fragiskatos: Thank you very much.

I think that's three minutes.

The Chair: That is three minutes.

Mr. Peter Fragiskatos: The chair is smiling, which usually means yes.

The Chair: You had 11 seconds, but that's fine.

On behalf of the committee, I want to thank Mr. Jacksch and Ms. McPhail.

I'm going to suspend until we reconvene the meeting.

● (0940)

(Pause)

● (0945)

The Chair: Let's bring this meeting back to order.

Our second set of witnesses is from the Department of Citizenship and Immigration.

I am going to call on Mieke Bos, the director general, and ask her to introduce the people she is with.

I've already told our witnesses that this will be a 55-minute session rather than a full hour because the committee has five minutes of business to do.

With that, go ahead, Ms. Bos.

Ms. Mieke Bos (Director General, Admissibility, Department of Citizenship and Immigration): Mr. Chair, good morning.

Members of the committee, good morning and thank you for inviting me here today to discuss the entry-exit initiative, as Bill C-21 is now in second reading and being studied by this committee.

[*Translation*]

Thank you for inviting me here today to discuss the entry/exit initiative.

[*English*]

My name is Mieke Bos, and I am the director general for the admissibility branch at Immigration, Refugees and Citizenship Canada, IRCC.

The admissibility branch within IRCC provides policy support to the managed migration of visitors to Canada and protects the health, safety, and security of Canadians. We work very closely with the Canada Border Services Agency, CBSA, on a number of files, and entry-exit is just one of them. We liaise on an ongoing basis with the CBSA on migration control and security management, including admissibility, identity management, visas, travel documents, and information sharing.

● (0950)

[*Translation*]

I am accompanied today by two colleagues: Emmanuelle Deault-Bonin who is the director of Identity Management and Information Sharing, and Marc-Andre Daigle, director of Strategic Initiatives and Global Case Management System Coordination in the Operations section of the department.

[*English*]

As you will have heard earlier in the week from the Minister of Public Safety and colleagues from CBSA, as an entry-exit initiative partner, Immigration, Refugees and Citizenship Canada will receive entry-exit data from the CBSA to support its program objectives.

[*Translation*]

Building on what you heard, I would like to focus on the significance of the entry/exit initiative for Immigration, Refugees and Citizenship Canada (IRCC).

[*English*]

The essence of the entry-exit initiative is about information sharing, verification, and compliance. It is about knowing who enters Canada and who exits Canada at any given moment in time. It's about providing a complete travel history for those applying to be permanent residents or Canadian citizens. It is a system to share information between Canada and the U.S., so that a record of entry into one country becomes a record of exit from the other. The benefits of this initiative are important for my department as the entry-exit system will close a knowledge gap by providing objective information on movements into and out of Canada.

Canada has also committed to collecting exit information about the air mode by requiring airlines to submit a list of all passenger information on outbound international flights.

I cannot stress enough how access to this information will enhance program integrity across multiple lines of business by providing IRCC's officers with a tool to objectively confirm an applicant's presence in, absence from, entry into, or departure from Canada. I would underscore that this is not new. IRCC already collects travel histories from clients applying for citizenship or confirming permanent resident status.

With entry-exit records, however, IRCC officers would be able to verify the accuracy of information submitted by applicants, including their time spent inside and outside of Canada. This information may impact a decision on whether or not an individual qualifies for permanent resident status or being granted citizenship.

[*Translation*]

IRCC has been working closely with the Canada Border Services Agency (CBSA) to advance this initiative and plans to obtain entry and exit information from the CBSA to support its administration of the Immigration and Refugee Protection Act, the Citizenship Act and the Canadian Passport Order. The entry and exit information will also assist in case processing and identifying instances of fraud across IRCC's multiple lines of business.

[*English*]

For example, an individual's presence in or absence from Canada is a key requirement in the large volumes of applications and investigations processed annually in the temporary resident, permanent resident, asylum, citizenship, and passport streams. Taking it a step further, access to the CBSA's entry-exit information will provide IRCC decision-makers with an objective travel history to support the processing of an application or investigation. I will give you a few examples.

Accurate, objective entry-exit records will allow IRCC to strengthen the integrity of citizenship and immigration programs by being able to verify that those who claim to have resided in Canada and to have met the residency requirements have actually done so.

It will allow us to better identify temporary residents who overstay their allowable period in Canada. It will allow us to verify that sponsors in the family class are residing in Canada where required by law, and to verify relationships in compliance with conditions for spouses and partners applying or admitted in the family class. It will allow us to ensure ongoing entitlement to a Canadian travel document. It will allow us to support investigations into possible fraud in relation to immigration, citizenship, and passport travel documents, and to detect persons overstaying their visa and immigration warrant closures. It will also allow us to identify individuals who may have failed to meet residency requirements for permanent residency status or citizenship applications.

Moving on to privacy safeguards and concerns, IRCC has a strong privacy track record. As the holders of a vast amount of personal information, we are well versed in the legislative and policy requirements that guide the collection, use, and safeguarding of personal information. The existing privacy frameworks that IRCC has in place for its various business lines continue to apply.

I would echo the Minister of Public Safety's comment earlier in the week that privacy is an important component of the entry-exit initiative. IRCC will be submitting its own privacy impact assessment to the Office of the Privacy Commissioner for entry-exit, and updating its application forms and website to ensure that applicants are aware that the information on their travel history will be obtained from the CBSA to support their application.

● (0955)

[*Translation*]

IRCC takes its privacy obligations very seriously, and together with the CBSA, and the Office of the Privacy Commissioner of Canada (OPC), we will continue to work to ensure that privacy principles are upheld.

[*English*]

From a functionality perspective, IRCC would only query the CBSA's entry-exit database when processing an application or when conducting an investigation. For instance, IRCC would access entry-exit data when there is a program need, for example, to confirm that an individual has met the residency requirement for a grant of citizenship.

From a client perspective, the benefits of entry-exit information means that IRCC is able to make better informed decisions that impact the lives of those clients. IRCC will use entry-exit information to enhance the processing of legitimate applications and investigations into temporary resident, permanent resident, asylum, citizenship, and passport programs.

[*Translation*]

For example, entry/exit records would make it easier for IRCC to verify that residence requirements are being met by applicants for eligibility in citizenship and immigration programs. Access to entry/exit information from the CBSA will be used to strengthen current limited travel history information found in passport stamps, which may not always be available or add to processing delays.

[*English*]

Collecting the entry-exit records of Canadian citizens will enhance the integrity of IRCC citizenship, immigration, and travel documents programs. Entry-exit travel records would support provisions under IRPA legislation relating to sponsorship residency and verification of family relationships. Entry-exit information would support investigations concerning the revocation of citizenship and the misuse or abuse of Canadian travel documents such as the Canadian passport.

Members of the committee, as you can tell from my remarks, from an IRCC perspective we very much welcome your consideration of Bill C-21. The information that will become available to us once entry-exit is fully functional is important to the work of my department.

With that, I conclude my opening remarks.

Thank you again for the opportunity to be here with you today.

[*Translation*]

My colleagues and I will be pleased to answer any questions you may have.

[*English*]

The Chair: Thank you, Ms. Bos.

[*Translation*]

Mr. Picard, the floor is yours for seven minutes.

[*English*]

Mr. Michel Picard: Thank you. Your French is improving a lot.

The Chair: Yes, I know.

[*Translation*]

Mr. Michel Picard: Thank you all for your contributions and for being here.

First, I think one of the hot topics related to Bill C-21 is the information sharing. So, for the benefit of those following the discussions from outside, could you once again talk about the procedure you follow to obtain information and how you might use the information and pass it on, if applicable?

Is that possible?

Ms. Mieke Bos: I will answer in part, and perhaps I will ask my colleague Mr. Daigle to elaborate on the procedure.

[*English*]

In terms of exchange of information, there are two layers of exchange of information. There is the higher level exchange of information between Canada and the United States. That part, as you've heard earlier, Monsieur Picard, is in the hands of CBSA. They have an agreement with the United States. We are not directly implicated in that.

IRCC has an understanding, an arrangement with CBSA in terms of our accessing the entry-exit information once the system is up and running.

I have to stress though, that we already have the right to collect this information. This is not new. IRCC, under the Customs Act, has the right to collect entry-exit information from persons leaving and entering Canada. The entry-exit system will provide automatic...or will facilitate the access to this information.

● (1000)

Mr. Michel Picard: The access you have is what is actually exchanged. This is everything for Canadian citizens or U.S. citizens, but it is actually under the agreement.

Ms. Mieke Bos: Yes. Currently we don't have access to exit information. We can ask on a case-by-case basis, and of course, CBSA only has partial information at this point in time.

Mr. Michel Picard: Yes.

Ms. Mieke Bos: That is only what is collected at the land border and not from Canadian citizens.

Marc-André.

Mr. Marc-André Daigle (Director, Strategic Initiatives and Global Case Management System Coordination, Immigration Program Guidance, Department of Citizenship and Immigration): Thank you for the question.

[*Translation*]

Mr. Chair, let me clarify the issue a little and add to my colleague's comments.

In terms of legislative mechanisms or memoranda of understanding, there is

[*English*]

a statement of mutual understanding

[*Translation*]

and those mechanisms allow for the sharing of data between the two departments.

As my colleague explained, in terms of the procedure and the sharing of entry and exit information, the data will be taken from the agency. The development of the systems will enable our departmental officials to access information and send requests through those systems. This will make it possible to have a copy or a version of that information, which will be based on the criteria, or the biographical data, covered in the bill. This will also make it possible to check whether clients have applied in the past and whether we know them. As a result, we will be able to add information to the person's travel history.

Mr. Michel Picard: Once the information is sent, does it become your "property", to the extent that you have the discretionary power to either send or not send the information to a third party requesting it?

There are concerns that a provincial government or a provincial agency might contact you to request that information.

What happens there exactly?

[*English*]

Ms. Mieke Bos: To the best of my knowledge, we access the information from CBSA but only when we're processing an application, so it's IRCC immigration information. To the best of my knowledge, we do not connect with provinces on this.

Mr. Michel Picard: It stops there.

[*Translation*]

Ms. Mieke Bos: Ms. Deault-Bonin, do you have anything to add?

Ms. Emmanuelle Deault-Bonin (Director, Identity Management and Information Sharing, Admissibility, Department of Citizenship and Immigration): Yes, thank you.

The information supports an IRCC decision. It's a piece of the puzzle that we consider together with all the other pieces of the puzzle we have, whether it's the information provided by the applicant in their application or the information that we have gathered. We then make a decision.

Let me give you an example. If we receive a request for information on an individual's entry and exit, we will direct the requesters to the CBSA, which is, first and foremost, responsible for that data.

However, if someone asks us to confirm whether an individual is actually a Canadian citizen, we will take care of the request and answer the question. The agreement that Mr. Daigle mentioned helps to clarify the responsibilities, because we work very closely with the CBSA.

Mr. Michel Picard: Very well.

I'm sorry to interrupt you, but I don't have much time left. I have one final question, which is very important to me.

[*English*]

You mentioned that the entry-exit system "will close a knowledge gap". Did you mean completely or partially?

Ms. Mieke Bos: We currently do not have exit information, so we rely on our clients to provide that information. First of all, clients are not always good at keeping their own records. Actually, there's an initiative started in our client service departments whereby clients are going to get a little insert in their passport to keep track of their movements.

We rely on the information that clients provide us. This can be timely and cumbersome. Sometimes, for a citizenship application or for a permanent residency card, they have to submit secondary information to prove that they were in Canada. Most clients are bona fide and we have absolutely no problem trusting the information they provide, but there are people who are trying to defraud the system. At that point in time, we have to do a lot of work to investigate. This will just provide an objective non-disputed base of information, so it closes an important gap.

● (1005)

[*Translation*]

Mr. Michel Picard: Thank you very much for your time.

The Chair: Thank you, Mr. Picard.

[*English*]

Ms. Gallant, you have seven minutes.

Mrs. Cheryl Gallant: Thank you, Mr. Chair.

Right now there is a disconnect between your department and CBSA. Your website instructs people to validate a confirmation of permanent residence or permanent resident visa. If they live in Canada, they are told to go to a Canadian border if they can't get an appointment at an office near them.

People go to the border, but in order to go to a Canadian border agent, they have to travel into the United States. They're in the United States, for example, and then they provide their information or their application for permanent residency to the CBSA. The CBSA agent says they are there illegally, when the person is genuinely trying to follow the steps as set out in terms of getting a permanent residency card. They're left stranded. They have to get an airline ticket, go back, and then they face the prospect of never returning again, because of this disconnect.

How do we know that same disconnect that exists for people legally trying to apply for permanent residency isn't going to have grave consequences for law-abiding Canadians when this is implemented?

Ms. Mieke Bos: I have heard those stories with the scenario you are referring to, but this falls outside of my area of expertise. The entry-exit information will apply to everyone leaving Canada, which is information that we currently don't have. The purpose of this information is for us to establish whether the clients applying for permanent residency or citizenship have met the residency requirements. We are legislated to do that.

The committee will have followed the Bill C-6 proceedings. Bill C-6 will come into effect shortly, and it determines exactly what the residency requirements are for future citizens. As I explained before, currently we rely on the information from the client. The vast majority of clients are entirely legitimate, of course, but there are cases of abuse, so this allows us to objectively verify when applicants were in Canada and when they left.

Mrs. Cheryl Gallant: Okay, so let's look at people who are trying to avoid following the rules.

Instead of going to a regular border crossing, they're going to look for your weakest point. Aside from what we are seeing right now with the illegal crossings into Canada, there are several bodies of water between Canada and the United States, for example. Somebody can take a pleasure craft, go across the river at the Thousand Islands, and just decide not to check in. They are supposed to by law, but maybe they don't.

What sorts of safeguards or measures are you going to put in place to ensure that the most likely points of crossing for somebody who is trying to avoid being recorded as leaving Canada are captured as well in your data system?

Ms. Mieke Bos: The management of the borders is really the responsibility of the CBSA.

As IRCC, we're less well placed to comment on how CBSA would manage those scenarios.

● (1010)

Mrs. Cheryl Gallant: That would be incomplete data collection. It seems to me that if the purpose of the bill is to ensure that we know who's coming and going, even though it's CBSA, it should still be relevant to the immigration department to keep track of this.

Do the officials know why the data exit information is going to be shared with CRA? What is the rationale behind that, in terms of making sure we have legal immigration and we're keeping track of people for permanent residency purposes?

Ms. Mieke Bos: We focus on immigration-related purposes. The customs and collections aspect of this bill is of less immediate or direct relevance to the immigration department.

First and foremost, I would say that the benefit of this bill will be to establish residency requirements and to document overstays. Temporary residents, for example, are normally not allowed to stay more than six months on a normal visa or eTA. If they overstay in Canada, we will be able to establish that.

I don't believe that the immigration department is best placed to answer tax questions.

Mrs. Cheryl Gallant: Back to land borders that are non-official ports of entry, why or why wouldn't the information or that kind of data be useful in non-official ports of entry?

Ms. Mieke Bos: Again, the management of the border is CBSA's responsibility, but if someone enters Canada illegally, as we are seeing now, the system couldn't work because we wouldn't have an exit record and we wouldn't have an entry record. Only when the individual would be detained....

The system is intended to work at established border points, including airports in the air mode.

Mrs. Cheryl Gallant: The information would be helpful, though, if you had it at non-official points of exit or entry.

Ms. Mieke Bos: We rely on this information to establish residency requirements in different lines of business, so more information would be very useful for our purposes.

The Chair: Thank you very much.

Monsieur Dubé.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

My thanks to the witnesses for being here this morning.

As everyone knows, the program has been in place since 2013, but it only applies to people whose citizenship is other than Canadian or American, including permanent residents.

How did the collection of data on permanent residents unfold? Were there any problematic cases? Has it affected the records of any individuals since 2013, when the program started?

[*English*]

Ms. Mieke Bos: IRCC, since the initial rollout pilot project and partial rollout that the member of the committee refers to, has not yet had an automatic connectivity with Canada Border Services Agency, which is really what we will be establishing once the entry-exit system is up and running.

Currently, we don't have a way to access this information in a systematic way. If we need verification, we can go to CBSA on a case-by-case basis.

I may ask my colleague Marc-André to provide a little bit more clarity on how it works currently and how it will work in the future.

[*Translation*]

Mr. Marc-André Daigle: Great.

The first two phases of the entry/exit initiative, a large-scale measure, consisted strictly of memoranda of understanding and information-sharing protocols between the Government of Canada and the U.S. government. The exchange took place strictly between the IRCC and the CBSA. The Department of Citizenship and Immigration is very interested in monitoring and overseeing the progress of this initiative. However, unfortunately, I am not in a position to tell you about our department's active participation and the development of the connectivity.

● (1015)

Mr. Matthew Dubé: I want to make sure I fully understand what you are saying.

Since 2013, information has been gathered about the exits of Canadian permanent residents. Information is collected and shared, but your department does not have access to it. Is that correct?

Mr. Marc-André Daigle: I cannot comment on that. At this time, our department does not have access to the information systematically. However, as I explained, in cases where there are doubts about people or an investigation is initiated, there are memoranda of understanding for the exchange of data and information, as well as privacy measures. This allows us, at the federal level, to have protocols and to share data on a case-by-case basis.

Mr. Matthew Dubé: So it would be difficult to assess the potential impact on someone who has been granted permanent resident status and would like to obtain citizenship, for example.

We are not really able to tell whether the collection of information has had an impact on the file, because, in most cases, you would not have access to that information. Is that correct?

Mr. Marc-André Daigle: Actually, in the next phases, phases three and four, the exchange of information about all people travelling by land between Canada and the United States will be more systematic. In addition, the final phase will make it possible to obtain more information beforehand, from the manifests of travellers who leave Canada.

Once we have access to the various components, we will be in a better position to assess the short-term impact on cases where there are doubts about travellers regarding the

[*English*]

their requirements in terms of permanent residency.

[*Translation*]

Mr. Matthew Dubé: Are you in a position to tell us the number of suspect cases where the information would have been shared since 2013, when the program started? You can also provide us with this information at a later time, if you cannot do so now.

Mr. Marc-André Daigle: Unfortunately, I'm not able to give you that information.

Mr. Matthew Dubé: My next question is whether there's a recourse mechanism if someone challenges the information about them.

If there is a human error in a file that the Canada Border Services Agency sent you, is there a recourse mechanism in your department that allows the person concerned to correct the record?

[*English*]

Ms. Mieke Bos: There are existing redress mechanisms in all of our lines of business. The CBSA has its own redress mechanisms.

Let's say a permanent resident makes an application for citizenship and we deny it based on the information available, partially based on the information we obtain through the future entry-exit system. There's always a redress system. The client can always go back and contest, and a follow-up can be done. That exists throughout the department.

[*Translation*]

Mr. Matthew Dubé: I have a specific situation in mind about a constituent in my riding. She had bought a plane ticket to visit a family member abroad. My office intervened to warn her not to do so because of the potential consequences.

With the way the legislation is written, could such a case come to your attention, since the person is supposed to have left the country after buying a ticket, even though she did not end up leaving the country?

[*English*]

Ms. Mieke Bos: If I understood your question correctly, the moment that the information is made available is when the person is actually on the manifest. Even if somebody purchases a ticket, we would not have access to that information. It's the moment that somebody is on the manifest of the airline and the airline submits that manifest back to us. It's when somebody is actually departing the country.

[*Translation*]

The Chair: Thank you, Mr. Dubé.

[*English*]

Mr. Fragiskatos.

● (1020)

Mr. Peter Fragiskatos: Thank you very much, Mr. Chair.

To pick up on the question that Mr. Dubé just asked, you say there are redress opportunities in place. Could you go into that in specific detail?

Suppose someone wants to contest the accuracy of the response given by your department. What exactly can they do?

Ms. Mieke Bos: I'll ask my colleague Emmanuelle to provide a bit more detail.

Ms. Emmanuelle Deault-Bonin: Again what's important to remember is that when we are looking at an application, the entry and exit data would come into play to validate information that would already be provided by the applicant as part of the application.

When we look at the application, there are a number of factors and sources of information. It always depends on the type of application. For example, you can ask for judicial review and you have a right of appeal in certain applications. You also have the Privacy Act that allows you to seek access to your record and make corrections if there are issues raised. That's another avenue that clients can avail themselves of.

There is also procedural fairness built into some of the process. Prior to making a decision, there are mechanisms by which we can communicate with the client to say, "Here are some of our doubts and some of our questions. Can you provide more answers before we make a decision?"

There are different tools, depending on the type of application and the seriousness of the potential inadmissibility, but also through the privacy regime that we have here in Canada.

Mr. Peter Fragiskatos: Thank you very much.

Ms. Bos, in your written testimony that I have here in front of me, you state on page 8, "For example, entry/exit records would make it easier for IRCC to verify that residence requirements are being met by applicants for eligibility in citizenship and immigration programs."

To what extent is this a major challenge right now? Tell us how this bill can be helpful in dealing with that challenge.

Ms. Mieke Bos: Thanks very much, Mr. Chair, for the question.

It can be a challenge in certain cases just because clients aren't always good at keeping their own records, frankly speaking. I think that when we talk about the benefits of this system, we're talking about the benefits for the vast majority of entirely legitimate clients of IRCC, who may have forgotten when they went on holidays or came back, or who just have not kept their records properly.

Sometimes our officers have to spend a lot of time retracing the steps and seeking evidence that the clients have actually met the requirement. It's a facilitative tool in that sense, but of course it's also very important to make sure there are no fraudulent applications.

Mr. Peter Fragiskatos: Thank you.

On page 3 of your brief, you talk about a knowledge gap being in place now, which we've heard about already. I think Mr. Picard asked the question. Tell the committee, but also speak to Canadians on this. How does the knowledge gap that's in place hinder your work? How does it get in the way of good public policy execution?

The committee is here performing our roles, but we're here on behalf of Canadians. I think that if there's a knowledge gap that exists that's concerning, tell us specifically why it's concerning.

Ms. Mieke Bos: I think it's concerning, Mr. Chair, because it hinders program integrity; that's the term we use. We want to make sure that those who are entitled to citizenship and to permanent residency get it, and that those who are not entitled to it do not get it. I think it is in the interest of Canadians and of the country as a whole to make sure that the very robust immigration programs we have in place, which are fair, transparent, and clear, are adhered to.

Again, it is a matter of what we refer to as program integrity, so that the right people benefit from the programs we have put in place.

● (1025)

Mr. Peter Fragiskatos: Thank you. I have a final question.

On page 7 of your brief, it states, "IRCC takes its privacy obligations very seriously, and together with the CBSA, and the OPC, we will continue to work to ensure that privacy principles are upheld."

Can you talk about the coordination, specifically between IRCC and CBSA, and exactly how that unfolds on the issue of privacy?

Ms. Mieke Bos: Thank you for the question.

I will turn to my colleagues. Emmanuelle's daily bread and butter is identity management and privacy, so I may ask her to provide a little more detail.

Mr. Peter Fragiskatos: Sure. It's a much more complicated life than I lead.

Voices: Oh, oh!

Ms. Emmanuelle Deault-Bonin: It's a great question. Thank you.

One of the things that we do in collaborating with CBSA on privacy is to look first at doing privacy by design. When we're working together in enforcing and administering our immigration laws, how can we do this exchanging of information in a way that's necessary, relevant, and proportionate?

I think this is a good example in that, first, the data elements that we're sharing are minimal. It's really just what we need to answer the questions. As well, the way we do it is through a privacy lens. We're not diving into a database and just trying to make our way though it. It is through a query and response system, when we have an applicant in front of us and when we need it.

That's the work that my colleague and I do on a day-to-day basis, but we also, obviously, work together in engaging the OPC. They're a very important partner in providing feedback on those privacy questions.

The Chair: Thank you very much, Mr. Fragiskatos.

Mr. Motz, you have five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Mr. Chair.

Thank you for your attendance today. I just have a couple of questions.

Do you feel that the information you'll be collecting with regard to Bill C-21 will reduce IRCC's workload? If it reduces workload, will it also reduce costs?

Ms. Mieke Bos: Will it reduce workloads? We believe so. Currently we have to do a lot of this verification manually, and again, rely on the accuracy of the client's data keeping, if you like. Again, it can be quite a cumbersome process for our officers to verify and establish that the residency requirements, indeed, have been met.

To come to your point on cost savings, as always, once we enter into the regulatory phase, we do a cost-benefit analysis. I've seen some initial analysis, but I couldn't say, hand on heart, that this will be a cost-saving measure. I do know that it will definitely reduce the workload of our officers. We will go from a manual case-by-case, established sometimes on incomplete information, to a systematic verification of information.

I'll ask my colleague to elaborate.

Mr. Marc-André Daigle: In terms of the direct impact on cost, that's a very interesting question. I fully appreciate it, but it's quite complex in terms of being able to provide the metrics that support it. I would like to provide a little bit of the qualitative in terms of how this will have an overall impact through our entire processing network.

As you understand, we have offices in Canada and also all around the world. If I'm looking just in terms of the investigation clients where there are active cases, it can take place initially when an application is being processed overseas, but it can also make its way all the way through by the time the person is in Canada or there is information sharing between our different units. It's the time invested in building the case for the investigation, but also the cost of accessing that information. If it's a large-scale investigation, and there are more federal partners involved, then it adds to the cost.

I don't really have the breakdown. This was just to provide a snapshot in terms of the overall impact that will have.

Mr. Glen Motz: You alluded that there are some preliminary analysis or estimates. If it's possible at this point in time to provide those to the committee, that would be awesome. Thank you.

How will immigration and the CBSA go through correcting information that is discovered to be erroneous, and how is that going to be cross-referenced and shared? Is there any thought as to how that process is going to occur?

● (1030)

Ms. Mieke Bos: There's expected to be a very high degree of accuracy. Flight manifests are pretty black and white in terms of the information they provide. There will be automated systems at border exit points. Of course, there is always the possibility of an error, so the two organizations will be working together in case we come across faulty information.

Marc-André.

Mr. Marc-André Daigle: Just to add to that in terms of how it will work, if there is a conflict or erroneous information, in terms of taking a step back, when we're looking at the datasets that will be used or collected in terms of entry-exit, it is quite minimal in terms of the key tombstone information on page two of the passport, complemented by place, time, date, and location of departure.

In terms of making the identity management, in terms of reconciling our own historical client-based information, there is a potential that either.... If we look at clients who have common names, for example, there is a risk that there could be duplicates or a mismatch. Therefore, officers would be reviewing these and then making that determination, based on the historical information that we have, to see if they are the person or not. If they are not, then we would not retain that information. It would be purged.

The Chair: Thank you, Mr. Motz.

[*Translation*]

Mr. Arseneault, you have the floor for five minutes.

Mr. René Arseneault (Madawaska—Restigouche, Lib.): My thanks to the witnesses for being here today. Their remarks are very enlightening.

Ms. Bos, I have a practical question.

I see how the ease of access to the information on page 2 of the passport will benefit you. That's clear from this bill, which amends the Customs Act. I imagine that not all immigration and other claims come from the United States.

According to paragraphs 92(1)(a), (b) and (c) proposed in Bill C-21, the place of arrival in the United States must be disclosed. When you process all your applications, is the information that you would receive pursuant to paragraphs 92(1)(a), (b) and (c) about anyone coming from a country other than the U.S. relevant? If someone did a Somalia-Canada return trip rather than the U.S.-Canada, would that affect your investigations? How do you see that?

[*English*]

Ms. Mieke Bos: I hope I understand the question correctly and I apologize if I did not. Obviously, we already have the entry information. If a foreign national comes in by air, the person passes CBSA, so we have the entry information. What the system will now provide is the exit information, which is currently a gap. In most countries, in Europe and the United States, exit information is pretty systematically collected. Really what it helps us to establish is the travel history of the client. With the coming into force of this legislation, our colleagues at the border services agency will be able to collect this information at all entry and exit points, both at the land border and in the air mode.

Again, I hope I understood the question correctly.

[*Translation*]

Mr. René Arseneault: You understood the question correctly. Good job. It's true that it was poorly worded.

The CBSA will have the information about the exit of someone coming from Belgium, for instance, when they arrive in Canada, but pursuant to proposed paragraph 92(1)(c), it would not know their destination. Have I understood that paragraph properly?

[*English*]

Ms. Mieke Bos: This is correct, but for the purposes of this legislation it is not really relevant to us. What we need to know is whether the applicant was inside or outside of Canada.

● (1035)

[*Translation*]

If that person was in Belgium or Somalia, in terms of this bill, it would not concern us as much, if you will.

Mr. René Arseneault: The exit is what matters most for your investigations, correct?

Ms. Mieke Bos: Absolutely.

Mr. René Arseneault: Great.

The proposed subsection 92(1) refers to the sources from which the agency would collect the information, which it would then forward to you in compliance with proposed paragraph 107(5)(j), if I'm not mistaken.

Do you have any reason to believe that, somewhere in the world, there are sources that are not really reliable or is that not at all an issue for the agency?

[*English*]

Ms. Mieke Bos: This is written in a way to cover different sources, but normally this would be the passport. Page two of the passport contains the biographic information and that is what would normally be the source of the information. This is more about how our colleagues from the CBSA will handle this information.

Mr. René Arseneault: Yes.

Ms. Mieke Bos: What matters for us is what is entered into the system and that we then have access to it.

[*Translation*]

Mr. René Arseneault: Do I still have time, Mr. Chair?

[*English*]

The Chair: You have 30 seconds.

Mr. René Arseneault: From what I understand, the source is not the passport. The information comes from the passport, page two, but the source is maybe the foreign country, which provides the information.

[*Translation*]

Are sources from different places in the world just as reliable as the resources you have right now to find that information?

[*English*]

Ms. Mieke Bos: That is not affected so much by this legislation, but when we issue a visa to a foreign national, establishing the integrity of the document issued by a source country is a very important part of that process. That's the heart of the work that my branch does. It's the admissibility criteria, how we allow foreign nationals into Canada. It's based on the credibility of the passport and all sorts of information.

The source document, however, is something we take very seriously. That is not really part of this legislation, but it's something IRCC and our security partners take very seriously.

The Chair: Thank you very much, Mr. Arseneault and Madam Bos and your colleagues.

Before I suspend and reconvene in camera, on behalf of the committee, I want to thank you for your work. We appreciate it and it's helpful to the committee's deliberations.

Thank you again. The meeting is suspended.

[*Proceedings continue in camera*]