HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 079 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 24, 2017

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Tuesday, October 24, 2017

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, it's 8:45, so let's get started.

Our first guest this morning is Professor Wesley Wark, whom many of you will know quite well and who is in severe need of an umbrella—or was in severe need of an umbrella.

Professor Wark, you've presented to many committees, so you know how it works.

Mr. Wesley Wark (Visiting Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual): Mr. Chairman and members of the committee, I thank you for the invitation to appear and testify on Bill C-21, an act to amend the Customs Act. I'm going to read my remarks, in a desperate academic attempt to stay within your 10-minute time frame.

Bill C-21 provides statutory powers for the final phase of the entry-exit initiative. As the committee will be aware from previous testimony, the entry-exit scheme dates back to promises made under the Beyond the Border action plan agreed to in 2011 between Canada and the United States. Its provisions are, for now, Canada-U.S.-centric. The Beyond the Border action plan is the latest iteration of agreed schemes for post-9/11 border security, dating back to the safe border accord of December 2001. The Liberal government affirmed its commitment to the entry-exit information plan during a summit meeting between Prime Minister Trudeau and then U.S. President Obama in March 2016.

The entry-exit scheme has had a staged rollout since its first phase, which lasted from September 2012 to June 2013. It served to test the data exchange between Canada and the U.S. at select land border ports of entry. The second phase began in June 2013 for fuller land border crossing information exchange for third country nationals, permanent residents of Canada, and lawful permanent residents of the United States. The final stage of entry-exit, requiring statutory force in Bill C-21, would see the biographical exchange of information on all travellers, including Canadian citizens, at the land border, and the collection of biographical exit data on all air travellers, again including Canadian citizens, leaving Canada.

Biographical data acquired under Bill C-21 would consist, as you've heard, of the page 2 information from Canadian passports presented to Customs and Border Protection officials at U.S. ports of entry when crossing the land border. This information includes, as you'll know, name, nationality, date of birth, sex, and place of birth.

For the air mode, it would involve what is referred to as API/PNR, or advance passenger information/passenger name record, data provided by air carriers and air reservation systems for exit records for air travel. API data includes page 2 biographical passport data plus flight information. PNR derives from airline departure control and reservation systems, and varies depending on the collector. It can include type of ticket, date of travel, number of bags, and seat information.

The information flow that Bill C-21 augments is meant to be automatic. It would involve the passage of electronic data from U.S. CBP at land entry—U.S. entry data becoming Canadian exit data—in near real time. For air travel, it would involve the transmission of electronic passenger manifests from air carriers. All of this information would go to the Canada Border Services Agency for processing.

The backgrounder published by the government when the legislation was first introduced in June 2016 indicates that the entry-exit initiative is meant to serve a large number of objectives. It is not specifically a national security tool, but could, in my view, enhance investigations into the movements of suspected terrorists, foreign espionage actors, and WMD proliferators, among other actors of concerns, and it could provide a useful investigative supplement to other powers available to security and intelligence agencies.

It is worth noting that Mr. Bolduc of CBSA testified before this committee on October 3, making the point that one additional benefit that Bill C-21 powers would provide was “it will bring Canada on par with the rest of the world and our Five Eyes partners. There's a huge, huge benefit for Canada.” This was a direct quotation from Mr. Bolduc. I am not quite sure how to read this enthusiasm, except to say that Bill C-21 measures are, in keeping with a long tradition in Canadian national security, meant to demonstrate our ally worthiness.

In this same vein, it is also important to note the restrictions that the government has said it will put in place in terms of information sharing from the vast pool of data that will be collected under Bill C-21. Land border exit information will inevitably be shared with the United States government, because the information is collected by U.S. CBP agents. We are assured that exit information from the air mode would not be shared with the United States or any other foreign government. Whether this blanket restriction makes sense is questionable, in my view. The committee may wish to consider an amendment to the legislation in this regard, which would bring it more into line with the Secure Air Travel Act, of which I'll speak a little later.

Minister Goodale has testified before this committee that “exchange of information both within Canada and with the U.S. will be subject to formal agreements that will include information management safeguards, privacy protection clauses, and mechanisms to address any potential problems.” These are important promises that presumably will be fulfilled through regulation. Notably absent, however, is any commitment to transparency around the entry-exit initiative. There is no requirement, for example, for any annual report to Parliament and the public on its application and efficacy.

● (0850)

This lack of a transparency commitment is compounded by the current absence of meaningful independent review of CBSA, the core actor that will operationalize Bill C-21.

While government officials have testified that the information flows provided for through Bill C-21 will be seamless and automatic, the real issues, it seems to me, involve analysis of the data by CBSA, retention and security of the data, and information sharing. Bill C-21 legislation is a black box in these regards, leaving much to regulation. There is a question in my mind as to whether the legislation needs to be more forthcoming in three particular areas: data retention schedules, information sharing protocols, and transparency requirements.

Before I come to some modest proposals to improve Bill C-21, a note on a parallel and existing legislative power might be in order. There exists already a limited form of entry-exit controls for air travel, which have been in place since 2007 but which were amended with Bill C-51 in 2015 under the title of the Secure Air Travel Act or SATA. SATA, often referred to as the passenger protect program, creates a list of persons that the Minister of Public Safety “has reasonable grounds to suspect will (a) engage or attempt to engage in an act that would threaten transportation security; or (b) travel by air for the purpose of committing” a terrorism offence. I'm slightly paraphrasing the sections of SATA here.

SATA contains some provisions that are not held in common with Bill C-21, including specific powers and information disclosure, both domestically and through written agreements with foreign states and entities. These are under sections 11 and 12 of the Secure Air Travel Act. These sections, incidentally, are not proposed to be amended in Bill C-59 as that bill comes forward, presumably, to this committee.

There is also an important statutory reference to retention of data received from air carriers or air reservation systems in the SATA legislation, and this requires:

> The Minister of Transport must destroy any information received from an air carrier or an operator of an [air] reservation system within seven days after the act on which it is received, unless it is reasonably required for the purposes of this Act.

That's section 18 of SATA. In other words, the minister is empowered to retain records of air travel for the listed persons but not for the general public.

To bring Bill C-21 into closer alignment with SATA on data retention and information sharing protocols and to enhance transparency and ensure independent review of its powers, I would suggest the following responses to Bill C-21, which the committee might want to take under consideration:

First, Bill C-21 should adopt the explicit SATA references in sections 11 and 12 for information sharing domestically and internationally. I think this would be an improvement on doing this by regulation.

Second, Bill C-21 should adopt a reasonable retention schedule for entry-exit data based on expert government advice on the minimum period necessary for the retention to meet the many different objectives of the entry-exit initiative as listed in the backgrounder document published with the bill in 2016. A seven-day retention cycle as provided for in SATA would be self-defeating, but so would overly lengthy retention periods. CBSA must not become a data swamp.

Third, Bill C-21 should contain a mandatory requirement for annual reporting to Parliament on its provisions by CBSA.

Fourth, the committee should encourage the government to be explicit about its plans for the conduct of regulatory review of CBSA national security activities, either through an independent body or captured by the paragraph 8(1)(b) mandate for the proposed national security and intelligence review agency, NSIRA, under Bill C-59. This may require future clarifying amendments to Bill C-59.

Fifth, the committee should encourage the government to finalize its plans for an independent complaints mechanism for CBSA. There have been discussions under way about this for some considerable time now.

Sixth, and finally, I would encourage the committee to hold early hearings on CBSA and its rapidly expanding mandate. Doing so might serve as a foundational exercise for the new national security and intelligence review agency when it is created.

Thank you for your time and attention.

● (0855)

The Chair: Thank you, Professor Wark.

Mr. Fragiskatos, go ahead for seven minutes.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you very much, Chair.

Thank you, Professor Wark, for being here today. It's always great to hear your insights on security matters.

After the attack in Edmonton a few weeks ago, you were quoted in the press as saying, “Even lone wolves give off vapour trails that are potentially discoverable by security agencies.” The article goes on to say that you've advocated for a number of approaches to deal with such threats, better educating the public, and working with the Muslim community.

As far as our purposes today are concerned, you've talked about boosting the resources of security agencies. Legislation can be considered a resource in the fight against terrorism. To what extent does Bill C-21 provide CBSA and the Canadian state writ large with a resource to combat terrorism?

Mr. Wesley Wark: Thank you, sir. It's a good question.

I guess I would say that it is a tool. I think it's a modest tool. It's probably not important as some existing tools that have already been in place for some time, like the passenger protect program, for example. It's primarily an investigative tool. It would allow the tracking of individuals who might be of concern under the different portions of Bill C-21 . It would only be a supplementary tool. I don't see it as a magic bullet in any sense. I think it's a useful tool. It fills a gap. I don't think any government intelligence or security agency is going to look to it as a principal instrument. It's just a supplementary investigative technique.

Mr. Peter Fragiskatos: It's a tool in the tool kit, so to speak.

Could you comment about its utility from your perspective in dealing with fugitives on the run or in dealing with cases where children have been abducted? We've heard that the bill is helpful in that sense, but I would love your insight on that.

Mr. Wesley Wark: I'm sure it could be helpful, particularly in the sense that one has to keep in mind that, of course, it's not impossible to track through various existing means individuals who may be on the move and may be of concern for various reasons to the Government of Canada. You could do that through interactions with foreign partners, through organizations like Interpol, Interpol notices, and so on, but it's always nice to have your own. This is where I would put the benefit of entry-exits. It's always nice to have your own source of information about exit data so that you don't have to rely entirely on the assistance of foreign partners, at least in some initial tracking of where people might have gone. That requirement to be wholly dependent of foreign partners becomes more problematic the more difficult the foreign partner might be.

Mr. Peter Fragiskatos: Does this relate to efficiency? If a child is abducted, to use that example, would something like Bill C-21 provide Canadian authorities with the knowledge of when the child and the abductor had left the country? It would help to have that information on hand immediately instead of relying on the phone call across the border and waiting for a response from American authorities. This would speed things up and make things, as I say, more efficient.

Would you agree?

Mr. Wesley Wark: Yes, in theory at least, with a couple of provisos. One is that the information flow is going to be massive. In terms of the land border information exchange, it's not in real time. It's in near-real time. My understanding is that the CBSA officials will get batches of data on a kind of 15-minute cycle, but that remains to be seen because the full entry-exit initiative has not been tested. It certainly would be an advance.

The challenge, I think, is going to be in terms of how well CBSA is going to be able to digest that information flow.

● (0900)

Mr. Peter Fragiskatos: You said elsewhere in a CBC interview.... In fact, this came a number of months ago when the government was first proposing this sort of legislation. You said:

> There’s been a lot of concern over the years in Canada and elsewhere about data breaches where various malicious actors. You know, criminal groups, hackers, foreign governments are going after information held by the Canadian government and this big data base will be an attractive target. So, it will have to be properly locked down.

You touched on this in your presentation. I wonder if you could expand on advice on how we could properly lock down that information so it's not susceptible to hackers.

Mr. Wesley Wark: On that, I would say two things, sir.

One is that the Canadian federal government is in a good position in terms of data security protection, in the sense that it is able to call in the services of the Communications Security Establishment, which is well regarded as a cybersecurity organization.

The question then becomes the fit between what are going to be called the CSE's defensive cyber-operations and the CBSA's capability to lock down its data. We have that advantage. In part this is why I would encourage the committee to at some point take a close look at CBSA. If you look back at previous reports of Auditors General over a number of years, you'll see that CBSA has struggled with its electronic data and data systems, both at the border and at headquarters. It's not clear to me whether they've overcome those struggles or whether those struggles are going to become only worse as they're flooded with this kind of information.

I don't have an expert view at all on how well they're going to be able to manage that data flow. It's been tested to some degree, but not fully. I think it's certainly something that needs to have a watch kept on it. That's partly why, in addition to encouraging the committee to look specifically at CBSA, which is probably the fastest-growing, most expansive security and intelligence agency in the Canadian government, I would also encourage thinking around Bill C-21 that would require annual reporting on the impacts of the bill.

The Chair: Thank you, Mr. Fragiskatos.

Mr. Motz.

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

Thank you, Professor Wark, for being here.

In one of your last statements to my colleague, you indicated your concern with CBSA's ability to digest the information in that flow. The CBSA union president was here, I believe last week, and told this committee that they're currently facing a significant resource challenge, and he wasn't sure how this new bill was going to impact them. Obviously it's going to put more strain on the export of goods leaving the country. They now will be checking that as well as tracking people.

With these extra responsibilities, in your understanding of this, is there some concern that CBSA may not be able to meet the obligations of what the act is intending to do?

Mr. Wesley Wark: I think I would agree with the CBSA testimony that I've seen before this committee to the effect that the provisions of Bill C-21 will not make the border stickier in the sense of holding back the flow of people or goods. As I see it, the challenge is how CBSA at headquarters is going to be able to handle the data flow, and by "handle" it, I mean really two things: one, make sense of it, and the other, store it in some systematic way and secure it in some systematic way. I'm sure they have thought that through, but they haven't yet in practise met that full challenge, because they haven't seen the full flow of the data come yet.

The initial testing in phase one suggested that they were pretty capable of handling a relatively limited flow of data back and forth across the land border. Whether they're fully capable of handling both the land border exchanges and the exit air information I think is an important question that I don't have an answer to, but I think it's worth posing to them directly.

Mr. Glen Motz: Okay.

Earlier you made a statement about six or seven things you'd like to see being different in the bill. You referenced your first one, which is that there's a recommendation from your perspective on adapting the SATA references in the bill rather than in a regulation. Could you expand on that a bit more?

● (0905)

Mr. Wesley Wark: Let me just turn to SATA very quickly, if I could. There are short sections.

Section 11 of the SATA indicates:

> the Minister may disclose information obtained in the exercise or performance of the Minister's powers, duties or functions under this Act for the purposes of transportation security or the prevention of the travel referred to

Basically, that's indicating that this is a ministerial responsibility. It doesn't specify how exactly the minister may create regulation around domestic intelligence sharing or information sharing under C-21, but at least it puts the spotlight on the ministerial responsibility there, specifically with regard to domestic federal government information sharing. Given that there's a lot of concern around this and that it will likely resurface when C-59 comes into discussion again, some clarity in that regard would be important.

More importantly, from my view, the notion that we are going to create an entry-exit initiative for air travel and not share it with any of our close partners or any foreign state strikes me as a nonsense and something that is likely to be abused because it is a nonsense. I would prefer to see something like SATA section 12, which says:

> The Minister may enter into a written arrangement relating to the disclosure of information referred to in section 11 with the government of a foreign state, an institution of such a government or an international organization

It's setting down rules around how the minister can interact with foreign partners in the sharing of entry-exit data, which is the sensible way to go, rather than having a blanket restriction that will ultimately face pressure and potential abuse.

Mr. Glen Motz: Mr. Bolduc's enthusiastic statements seem to have been met with some skepticism on your part. Can you explain the genesis of that skepticism?

Mr. Wesley Wark: Skepticism may be too strong a word, and I deliberately didn't say I was skeptical about it. I just said I was puzzled by the degree of enthusiasm. "Huge, huge benefit" is a little over the top, frankly, in a couple of ways.

First, referring back to a previous question, this is a supplementary investigative tool. It's not going to change the view of our allies and partners about how well we perform security functions in Canada. It's not going to have a huge impact in that regard. Certainly it would be something that the United States government would look to see capped off, given the long history of this initiative.

Also, in the context of our recent discussion, if entry-exit information in the air travel or land travel modes is not going to be shared with foreign partners, I don't—to be honest—really see how this is going to be a "huge, huge benefit" for Canada, except to say we're doing it.

Mr. Glen Motz: In 2016, you were quoted in the *National Post* as noting that we may not be treated as an ally when dealing with the Americans and border control. Do you still hold that same fear with Bill C-21?

Mr. Wesley Wark: No. My fear is perhaps shared by many, and it's a fear about where the current American administration is heading on border security and a whole number of issues, like its unpredictability and the fact that it doesn't, at the moment, at least, appear to look at Canada as a very close ally and partner.

Mr. Glen Motz: Last, sir, I want to go back to the first point Mr. Fragiskatos brought up, on CBSA's ability and all the data that's available there. As I see this, one of the keys to the collection of this data is, as you put it, the analysis of it. You indicated that there might be some touchpoints with CBSA's ability to even manage the flow of it, let alone the analysis of it. What's your take on what that needs to look like from an analysis point of view?

Mr. Wesley Wark: Very briefly, Mr. Chair, the key here, as you say, is an analytical capacity for CBSA. CBSA, over the years since it was created in 2004, has been growing in intelligence analysis function, but it's still relatively small, untested, and immature. If they're going to have this volume of data, they really have to have a strong intelligence analysis capability, which goes way beyond algorithmic applications and is about human talent and interaction with the rest of the security intelligence community. That's another untested part of CBSA.

● (0910)

The Chair: Thank you, Mr. Motz.

Mr. Dubé, for seven minutes, please.

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

Mr. Wark, thank you for being here.

I want to understand what you're saying about the regulatory power, because a lot is left up to regulatory change. Essentially, would the part of SATA you just went through be to replace that regulatory power?

Mr. Wesley Wark: No, Mr. Dubé. It would clarify it in two particular ways. It would clarify that the minister would be responsible for any sharing arrangements that were undertaken using this data coming in to CBSA with other federal government departments. That would obviously intersect a bit with SCIDA provisions of Bill C-59, which will come up before this committee.

The more important part in my view is to allow the information collected through this initiative to be shared under written agreements that would be composed by the minister to be shared with select foreign partners. Those are the section 12 provisions of SATA.

Mr. Matthew Dubé: That's great.

On the question of the annual reporting that you spoke of, would it be appropriate, do you believe, to amend the law to have a statutory obligation to provide annual reporting, say, to Parliament, for example?

Mr. Wesley Wark: The short answer to that is absolutely. It seems to me it would fit nicely under the current government's transparency commitments. As you know, in Bill C-59 there are a variety of statutory requirements for agencies to provide public reports, and in some cases unprecedented public reports to Parliament and the public, for example from CSE. I think this would be very appropriate to build into Bill C-21.

Mr. Matthew Dubé: That's great.

We talked about different words that are used that sometimes mean the same thing, depending on who's saying them: an independent complaints body or a watchdog or even a redress mechanism, and sometimes they don't. They're not always synonyms, but they can be, depending on what issue you are attempting to address.

I want to get your thoughts on that because one of the issues that came up with government officials from Immigration, Refugees and Citizenship and also from Employment and Social Development was that essentially the redress would be with them, so one of the stated objectives being for people vying for citizenship or people who are on EI and so forth. In those situations, do you believe there should be a redress mechanism directly with CBSA to contest the accuracy of the information that's being collected?

Mr. Wesley Wark: Monsieur Dubé, I would say that internal resolution mechanisms may be helpful but are always inadequate, so there is a need for independent handling of complaints, and there has to be a triage process to make sure that those complaints are serious. That can be built into the law.

To go back to part 2 of Justice O'Connor's report on the review of the RCMP's national security activities, he proposed at the time, in 2006, that there should be a new, independent complaints mechanism for the RCMP and CBSA combined. So far we haven't seen how the current government intends to proceed with any kind of independent complaints mechanism for CBSA. Such a thing is necessary, whether it's combined with another body and operated by CRCC, or however it's done, as a whole-of-government complaints mechanism of some kind. That's all open to debate, but something has to be put in place.

Mr. Matthew Dubé: The committee of parliamentarians and what's being proposed in Bill C-59 is the first time we're seeing any kind of review for CBSA. In that context, if I'm not mistaken—I just want to make sure I'm understanding correctly what's being proposed—that would only be for issues related to national security. Is that correct?

Mr. Wesley Wark: That's correct, although national security, as you'll know, Mr. Dubé, is not defined anywhere in the law, so the definition could be stretched or compacted, depending on the need.

Bill C-59 doesn't specifically indicate that CBSA, as one of the principal security and intelligence agencies, would necessarily fall under the systematic review of the new National Security and Intelligence Review Agency. The only agencies that are listed in part 1 of Bill C-59 are CSIS and CSE, and the rest is left to a broad mandate where CBSA and others might be reviewed, but not necessarily.

Mr. Matthew Dubé: I only ask the question because, with regard to Bill C-21, a lot of the reasons the information may be collected are arguably not for national security purposes when you hear the stated objectives of the bill. In that sense, would it be fair to conclude that these activities would not necessarily be subject to the review by these different bodies?

● (0915)

Mr. Wesley Wark: I think that would be a matter of experience. I take your point. My argument would be, hypothetically, that the most serious ways in which entry or exit information might be used probably bear on national security matters, although not always. It could be human smuggling and child abduction cases, and so on. The repeated matters of concern are likely to be in the broad national security field so that if you have some kind of review system in place for CBSA that primarily focuses on national security, my guess would be—and it's just a guess—it would capture most of what you really want to have reviewed.

Mr. Matthew Dubé: The last point I want to get to is data retention. You said this should be left to experts, people like the Privacy Commissioner and so forth. Would it be fair to say that there should be more explicit schedules for retention of this data?

Mr. Wesley Wark: Absolutely. We're seeing this come forward, and I again refer to Bill C-59, which isn't yet before the committee, and some other aspects around CSIS data analytics and so on. I think this is crucial for public confidence. It's crucial for the organization of CBSA itself. I think when vast amounts of data like this come into the holdings of an organization like CBSA the default is to keep it forever, just in case. I think that's a bad default kind of response. I think there should be a very strict retention schedule built into the legislation that would distinguish between the vast bulk of innocent information, which should be disposed of quite quickly, and information that might be concerning, that could be retained for a longer period of time. I think that should be part of the legislation, not left to vague regulation that we might not see.

The Chair: Thank you, Mr. Dubé.

Madam Dabrusin.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): It's been very interesting to hear you talk.

I'm going to pick up on a few things you've already been speaking about with Mr. Dubé. I was curious about the annual reporting piece you were discussing. To get a better sense, what would you be looking for in such types of reports, and how would you see it spelled out in the legislation, if that were going to be added in?

Mr. Wesley Wark: I think all you would need in the legislation is a requirement for an annual report to Parliament. Then Parliament, on the basis of annual reports, could decide how satisfied or not they were with them. I think the main substance of such a report would partly be statistical—what is the information flow and how effectively is it being handled. Some part of that annual report should refer to the value of this initiative and provide cases—without providing the details, necessarily—where it has paid off, really to prove that this, on top of all kinds of other measures we've taken since 9/11, is a valuable instrument. So it's efficacy, plus propriety around how the initiative's powers were being used.

Ms. Julie Dabrusin: Fair enough.

My understanding is that we've been collecting this kind of information already with respect to foreign nationals and permanent residents, so there's already an existing scheme. I was wondering if you've had a chance to look at how that has operated. Do you have a sense of what's been working or not working with the system that is already in place?

Mr. Wesley Wark: It's a good question. There is some publicly available information, particularly around the first phase of the rollout of entry-exit, where they were wanting to test how well they could digest relatively limited flows of information from the United States. There was statistical data provided, percentages of data that could be resolved relatively easily. Those looked good. Again, I think it would take someone more expert than I in what those statistics really meant to read them. I think the key thing to understand is that in addition to that sort of result in the first phase test and the privacy impact assessment in stage two, which has been released, we're just heading into new territory in terms of additional information and, in a way, more sensitive information on Canadian citizens that will be added in with Bill C-21.

Ms. Julie Dabrusin: So far, there are no specific flags that you would be able to raise for us, based on our past experiences of the previous system.

Mr. Wesley Wark: So far so good, it would seem.

Ms. Julie Dabrusin: All right. I was just trying to get a sense of that.

The Canadian Civil Liberties Association in some of their evidence had suggested adding reference to the charter in the preamble. Would that add anything or would it be purely symbolic?

● (0920)

Mr. Wesley Wark: You may have provided your own answer to the question. The CCLA has taken this approach to a number of pieces of national security legislation, arguing that a specific reference to the charter should always be built in. I can see its symbolic value. I also think, in strictly statutory terms, it's unnecessary, because the charter is the law of the land. It really is a matter of symbolic politics and up to parliamentarians to decide whether they feel that's necessary or not.

Ms. Julie Dabrusin: Thank you.

Talking about the complaints procedures, one of the things we've also raised in prior evidence is if there are errors with the information collected, how that gets reported back. You've referred to what the recourse procedures are as well, what's a review. They're slightly different. In fact, how do you say this information that's been collected is an error? Also, what if somebody wanted to contest how long information had been held, saying they felt it had been held too long or it shouldn't have been held? First of all, would you see that built into this legislation? You've been referring to Bill C-59 a fair bit. Do you see it built into another piece of legislation, and what would that look like?

Mr. Wesley Wark: I think I would just reference the fact that the government has been working on a complaints mechanism for CBSA. From my personal perspective, for what it's worth, I would give them time to work that out. They have consulted with outside experts and so on about how that might work. Hopefully, it won't be too long before we see what they're proposing. Then Parliament will have its say on that.

On the independent review of CBSA, my concern is just to kind of leave it vague, as part of a potential responsibility that might fall to the National Security and Intelligence Review Agency under Bill C-59, without CBSA being specifically referenced. Given the important role that CBSA is now playing, I would prefer to see it listed in the legislation somewhere that it will be subject to an independent review by somebody.

Ms. Julie Dabrusin: When you say “in the legislation”, are you talking about Bill C-21? I'm just trying to clarify it. Right now we're doing a review of this statute, and I want to make sure we're not....

Mr. Wesley Wark: Yes. It would be a crosscutting provision. It's really a timing matter, in a way. I think legitimately it should be in Bill C-59 and then referenced back to Bill C-21 in terms of coming-into-force provisions. Probably you folks around the table are more expert than I would be on how to manage that process. It should be in legislation somewhere. There could be a reference in Bill C-21 to that, cross-referencing another piece of legislation, I would think.

Ms. Julie Dabrusin: That's helpful. Thank you.

I don't have much more time here, but we were talking about the retention of information. That has come up a couple of times. You said that you would prefer it not to be left to regulations but to be within the statutes. You referred the SATA timelines but said they might be too short. Do you have any other reference points of what we would be looking at as proper timelines? What would be the references that we would look to?

The Chair: It will have to be a brief answer, please.

Mr. Wesley Wark: Okay.

It's very difficult, because generally, up until very recently, we haven't seen such timelines. Governments of various stripes have been very reluctant to do this. They prefer the flexibility of having non-public retention schedules. It's often treated as a national security matter and a matter of secrecy to do so. I don't think that's necessary in this case.

The challenge here, and I think the reason that the government would prefer to have this in regulation, is that there are so many different objectives to the Bill C-21 initiative that might require different kinds of timelines around data retention. Despite that, I would still say that I think you could outline the different objectives and say the appropriate retention schedules for each of these different objectives, with some caveat around flexibility, should be x. The basic idea, as that concept might be worked through, would not be to just let this information sit forever, which is, I think, the default.

The Chair: Thank you, Ms. Dabrusin.

Ms. Leitch, welcome to the committee. You have five minutes.

Hon. K. Kellie Leitch (Simcoe—Grey, CPC): Thank you very much, Mr. Chair.

Thank you very much for presenting this morning, Professor Wark. Thank you as well for your public service on the advisory council on national security from 2005 to 2009. It's greatly appreciated when Canadians of your stature step forward to provide that public service.

● (0925)

Mr. Wesley Wark: Thank you.

Hon. K. Kellie Leitch: My questions have to with what you were speaking to with respect to regulations. Having had the experience of developing legislation and then dealing with the regulations, you're correct that we often don't have that degree of transparency. You spoke a bit about the retention of data and having a schedule. It would be helpful to know what you think the specifics of that schedule would be.

As well, with respect to information-sharing and transparency, what are some of those details that you think should be considered for the legislation as opposed to regulations? If the government chooses not to place it in legislation, give us some direction on what those regulations should be. Obviously, those will be hashed out at some point in time.

Mr. Wesley Wark: Sure. Thank you, Ms. Leitch.

On the transparency part first, I think that's the easiest one in terms of building a requirement in the legislation that there should be a public annual reporting to Parliament on the performance of Bill C-21. It would be one of the occasions on which CBSA would come before Parliament to really explain how they're performing. I think that would be important.

The retention schedule is, I think, a very complex issue. I don't have an easy answer for you. I have gotten as far as thinking, I must confess, that it would be important to have in the legislation guidelines on retention, with some degree of flexibility, geared to the specific different objectives as outlined in the backgrounder.

If I were looking for a timeline around this, I would say one to two years, maximum, and differentiated among the different objectives—but not 15, not 30, not 75; not an eternity.

Hon. K. Kellie Leitch: My colleague Mr. Motz brought forward the issue of the need for analysis, and you raised this as well, and the degree of our current capacity to do this analysis, whether it be at the border, whether it be the RCMP, or whether it be other agencies. What do you think are the three or four key components of analysis that have to be done now but are not being done?

Mr. Wesley Wark: Thank you. That's a great question. I'm always delighted to have any chance to talk about intelligence analysis as a function of government, because I think it is completely underrated and under-resourced, and this is a historic problem of long standing. We have a very small analytical capacity in the Canadian security and intelligence community. Most of the resources go to collection, which is not an uncommon phenomenon among security and intelligence agencies.

The problem for Canada is that there are certain key agencies that essentially hoard analytic talent for good and obvious reasons. So CSIS, the RCMP to a degree, CSE, and the Privy Council Office hold the talent pool. The talent pool is a key. CBSA is a newcomer. It doesn't really have access to that talent pool, which is very carefully guarded by the existing organizations. To the extent that they need to have a very significant analytical capacity—and I think this is the case—they don't currently have the talent to do that. They don't have the organizational structure. They don't have the interconnectivity with the security intelligence community. They don't have the resources.

I used to serve on the advisory committee to the president of CBSA in its first years from 2006 to 2010, I think it was. I always delighted in the remark of the first president of CBSA, who said that for every three dollars he had—he never had three dollars, as far as we can see—if he could, he would spend two on intelligence and analysis. But that has never happened for CBSA or any other organization.

Hon. K. Kellie Leitch: Do you think that's just a product of funding, or do you think it's also about developing that talent pool within our own borders? We see, in the basics of just the trades in this country, a lack of talent. What are those things that we should be doing to foster that talent? You say there are pockets of it throughout our government, but obviously there's a need for a larger number of individuals in totality, absolute numbers, to be able to do that. This shouldn't just be about dollars, but how do we deal with that talent pool?

Mr. Wesley Wark: It's about recruitment. It's about training. Doing intelligence analysis well is a real professional skill, and it should have a professional career attached to it, which isn't really the case in the Canadian federal government system at the moment, though there have been many efforts in that regard. Training is better; there is some training now. Recruitment is a little more systematic. But it's been a slow process and it's very, very incomplete. Some agencies, I have to say, have been on the outside of those initiatives, and I would put CBSA in that basket.

The Chair: Thank you, Ms. Leitch.

Go ahead, Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you very much, Mr. Chair.

Professor Wark, it's nice to see you again. Thank you for being here and providing your expertise.

I represent a riding just south of the Pearson airport and less than an hour away from the Niagara region land crossing. People in my riding are travelling to the U.S. extensively. We have snowbirds, we have students, we have business travellers, and we have vacationers. There's great interest, both in the efficacy side of the bill that you described and also in the privacy side.

I want to start by taking you back one more time to the question of how we set the line for the retention of data and put to you the cases of human trafficking and amber alerts, where in some cases, it may take quite some time until it's evident that there's a trail across the border. Without putting a number on it, would you agree that this is one of those policy objectives that should be most influential in deciding how to structure the retention of data when it comes to missing persons going across the border and being exploited, abducted, and potentially subject to other crimes, as well?

● (0930)

Mr. Wesley Wark: Mr. Spengemann, thank you.

My answer to that question would be yes, absolutely. But I think it also reinforces at least my sense that what we're dealing with, with those kinds of cases in particular, are matters of immediate concern and emergency measures, if you like, where you want to have the ability to track exit as quickly as possible. Coming back to retention schedules, it's not that you would need to hold that data for a year or two years. You need it right away, and you probably don't have to hold it for very long because it will ultimately be supplemented by all kinds of other information for law enforcement and prosecutorial purposes. Yes, it's very important, but it's really real-time information that you need to deal with those kinds of cases, and reflecting on retention schedules, it probably doesn't provide an argument for lengthy retention.

Mr. Sven Spengemann: Thanks very much for that.

I wanted to take you to a different area of the bill that you haven't had a chance to discuss this morning. That's the inspection of goods leaving the country. That's proposed new subsection 95(1).

Canadians travel to the U.S. often with goods in tow. Students will study in the United States. Seniors will go to Florida with goods. The government has introduced legislation to legalize cannabis. What are your thoughts on the provisions dealing with the exportation of goods? You talked about the fact that the border would not be sticky, and yet we've got discretionary powers in the bill whereby an officer may, at his or her discretion, question somebody leaving the country. How do you see that evolving?

Mr. Wesley Wark: In a way, it's a challenge in Canadian-American relations, rather than a challenge for strictly Canadian border enforcement provisions. I think this is particularly true with regard to the legalization of marijuana. How that would be treated across the border is an issue that remains to be seen.

Again, I don't see in Bill C-21 measures that are going to make the export of goods or the movement of people more difficult. It's a question of how exit is going to be handled by the United States, particularly across the land border.

Obviously, we need to work very closely with the United States and try to convince them of the Canadian interests in this regard, but ultimately that will depend on their approaches.

Mr. Sven Spengemann: I take it, then, that you have relatively little concern with the fact that, under the legislation, an officer has the discretion to question a traveller. The language is "may collect... information".

Does that give rise to any other risks, in terms of profiling or some other concerns with the application of the legislation?

Mr. Wesley Wark: It doesn't give rise, in my mind, to significant concerns, insofar as that discretionary ability is surrounded by other strong protections in the law, not least the charter, and one hopes that it would be exercised in a common-sense way.

Where it comes back into play, in terms of our conversation, would be, again, in the importance and value of an annual report, which would detail problems of that kind, and the importance of an independent complaints mechanism to handle specific cases.

Mr. Sven Spengemann: Very quickly, in the remaining 30 seconds, what are your views on the retention of data or the collection of data for the purposes of enforcing the Old Age Security Act? As you know, we have a lot of seniors who spend time in parts of the U.S.

Do you have any concerns there from a privacy perspective or from a policy perspective?

Mr. Wesley Wark: I am inclined to be frivolous about this—I know I shouldn't. I am now a senior myself, officially, although somehow I don't get to travel to Florida. I would hope that a Canadian value of common sense and moderation would kick in on this. I appreciate that we are leaving it to regulation. I can't see the value of spending a lot of resources and penalizing seniors in terms of OAS benefits. It's probably only a small category of seniors who are able to collect those benefits anyway, and they are probably not people who have the ability to travel regularly to Florida and so on.

● (0935)

The Chair: Madam Gallant, welcome to the committee again.

You have five minutes.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): I believe that Dr. Leitch was going to start, and then if there was time left over, I would get it.

Hon. K. Kellie Leitch: I just have one quick question in follow-up to what we talked about before, with regard to data and analysis. Like you, I am a professor. Collecting a whole bunch of data, putting it in a data sheet, and not doing anything with it is not really valuable.

If you were going to do an allocation of data collection—which we do a great job of, but don't seem to act on, in government—versus the analysis component, which is for action that would benefit Canadians, what would be the allocation of resource funding and human resources for data collection versus analysis and implementation?

Mr. Wesley Wark: Dr. Leitch, thank you for the question.

My simple answer would be that the technological cost of data acquisition is coming down dramatically, virtually every minute of our lives. What has not changed is the challenge of making sense of that data, although there is always a kind of technological impulse to assume that there is some perfect equation, an algorithmic equation that's going to solve that problem for you.

I think the challenge is, in the face of the lowering cost of the technological component, to boost expenditure on the human talent that you need to say, "I have this pool of information on a computer in front of me, and I have systems that are screening it. Nevertheless, what am I making of this?" It's really the human talent part of the analytical challenge that I think is the most important. That requires a good analytical capacity—again, to come back to the things we talked about—human talent plus an organizational structure that makes sense.

Hon. K. Kellie Leitch: Would you say, then, a 1:3 or 1:4 ratio?

Mr. Wesley Wark: I would say 1:10—one to the technology, 10 to the human element.

Hon. K. Kellie Leitch: Very good. Thank you.

Mrs. Cheryl Gallant: I have a quick question, and then I'm going to pass the rest of the time to Mr. Motz.

One of the agencies that the data is going to be shared with is the Canada Revenue Agency. In terms of the purpose of this bill—protection and public security—what role do you see the CRA having in this capacity, having access to this data?

Mr. Wesley Wark: I'm sorry, but I'm not an expert on the CRA's functions. I assume it has to do with keeping a watch on individuals who are not complying with Canada's tax laws, but I'm kind of at sea about this. I just pay my taxes.

Mrs. Cheryl Gallant: That's not public safety or national security. Okay. I'm sorry.

The Chair: You have two and a half minutes.

Mr. Glen Motz: Thank you.

Professor, I was very pleased to hear your comments on the analytical capacity or the lack thereof and the need for it in government. I think my colleague across the way would agree with me, based on his background as well as mine, that it's absolutely critical. It's emerging that the most critical component in the public safety, law enforcement, and anti-terrorism environment in which we live in our world is the analytical capacity to review and track individuals. I thank you for that. I think it's something that CBSA will work with government to increase.

You indicated that part of your concern was with the appropriate retention schedules. That's complex. There need to be some guidelines with regard to those, along with some flexibilities. I guess I'm left to wonder about this, given my background. When data is redacted, is gone, or we lose it to a retention schedule, it's amazing how many times we require that data and we no longer have it. I'm thinking of the recent example from Edmonton. If that data had been lost some way, how would we know and how could we track some of the concerns we have regarding public safety and terrorism, which is what Bill C-21 is supposed to do?

I know some balance needs to be struck and I know there are some groups that would have us be more concerned about retention and say we should destroy everything within years. You indicated that there are some streams, and that, depending on the purpose, we need to have different retention schedules. Can you explain that so it's a bit clearer and so we get it right?

Mr. Wesley Wark: I'll do my best on this. Again, I don't feel I have any kind of perfect or solid answer for the committee on this, but I think the approach is to stream it according to the different objectives of Bill C-21 in terms of the concerns that it's meant to deal with, and to keep in mind as well that Bill C-21 information, entry-exit information, is going to be only a small piece to a larger informational puzzle that you might need to apply to particular cases. It's never going to be stand-alone information.

In that sense, although I understand your concern that once you delete data from a database it's gone forever, I think there are a couple of things to be said about that. One is that there's probably another source from which that data could ultimately be acquired if you really needed it after a period of time that was covered by the retention schedule.

Second, and importantly, we have to understand that the more that an agency like CBSA is flooded with information, just as a general proposition, the less able it's going to be to actually winnow that information and find what it really needs to find in it. My concern is with the way we can—

● (0940)

The Vice-Chair (Mr. Matthew Dubé): Professor. I'm going to have to ask you to wrap up.

Mr. Wesley Wark: That's okay.

The Vice-Chair (Mr. Matthew Dubé): I was trying to let you finish the thought there. It's an important one.

Mr. Fragiskatos, go ahead, please.

Mr. Peter Fragiskatos: Mr. Chair, I will be splitting my time with my colleague Ms. Damoff.

I want to go back, if I can, to the question about information about citizens being collected and the need to lock it down. Criminal groups could access it—hackers or foreign governments. It's back to that point again.

Our Five Eyes allies have similar legislation on the books. Canada is the only country, as even you have emphasized in the media, that does not have this sort of legislation in place. Are there examples you could point to, safeguards those countries have put in place, to address the fear you've highlighted?

Mr. Wesley Wark: I think it would be hard to find examples of purely successful data retention.

Mr. Peter Fragiskatos: I mean best practices or—

Mr. Wesley Wark: I think everybody is working according to the same best practices in terms of secure data storage and surrounding it with privacy protections. That would certainly be true for all of our Five Eyes partners, but really the challenge grows exponentially with the more information you have that you're trying to secure.

To come back to Bill C-21 information, particularly about Canadian citizens, it is basic biographical information, so to that extent, it's mostly publicly available information. It's probably important not to exaggerate our concerns about locking it down in specific terms, but there should be more concern with the principle, which is that any database needs to be protected.

There is passport information and, with regard to air exit, some more specific information that could be of value. There's the general principle that anything that comes into the federal government needs to be treated as data to be secured, and the question of whether CBSA can do that effectively given the vast volumes. The specific harms that might flow from hacking into this database are hard to measure, generally because those kinds of hacking attempts aren't specifically targeted at, say, this pool of data, but are used to gain entry into other pools of data. That's really how the most sophisticated hacking works.

Mr. Peter Fragiskatos: Thank you very much.

I'll turn it over to my colleague.

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

Thank you, Professor Wark.

I understand that Statistics Canada already publishes entry information for people coming into Canada, as well as their country of origin, so in terms of annual reporting, would it make sense to just have StatsCan add the exit information to their annual report, as opposed to producing a brand new report? If so, do you think it would make sense to make the amendment here, or in Bill C-59?

Mr. Wesley Wark: Thank you, Ms. Damoff.

I am not completely aware of what Statistics Canada does with this information or how regularly it reports it. I still think there would be value in putting a requirement into Bill C-21 legislation for an annual public report, without specifying exactly what should go into that. I think a statistical component would be important, partly just to demonstrate that CBSA is completely confident of its ability to acquire these statistics and to demonstrate them themselves. That would just be a basic test that they would be under.

Ms. Pam Damoff: I have another quick question.

Do you see any value in adding to this bill a clause that would require a review of the legislation after a certain number of years?

Mr. Wesley Wark: Ms. Damoff, I actually thought about that. It's very much up to members of Parliament to decide on that.

I suppose my personal view, for what it's worth, is that Parliament has a lot of onerous duties around reviewing bills on a schedule. If there had to be a trade-off to building in a scheduled review of this act as opposed to Bill C-59, for example, I would rather see it in something more significant, like Bill C-59, than this one.

It's a fairly limited bill in some respects, and if there is that parliamentary reporting requirement, I think that would go a long way to meeting any concerns and would not necessitate a review. If the public reporting suggested there were major problems with the initiative, then presumably Parliament could take some action.

● (0945)

The Chair: Thank you, Ms. Damoff.

Thank you, Professor Wark. It's always good to receive the wisdom of seniors.

Voices: Oh, oh!

The Chair: With that, we will suspend.

● (0945)

(Pause)

● (0945)

The Chair: We will bring this committee back to order.

We have two witnesses for our next hour. From the American Civil Liberties Union, we have Esha Bhandari.

I'm hoping you can hear and see me. After you hear and see me, it really improves.

Solomon Wong is an executive board member from the Canadian/American Border Trade Alliance.

Given the vagaries of technology and the importance of what you want to say, my suggestion, Ms. Bhandari, would be that you go first for your presentation.

Ms. Esha Bhandari (Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union): Thank you very much for having me.

I am Esha Bhandari. I'm a staff attorney with the American Civil Liberties Union, and I'm based in New York. I previously testified before the Canadian House of Commons committee on Access to Information, Privacy and Ethics on June 15, 2017, when I addressed two issues affecting Canadians' privacy rights in the United States' border searches of electronic devices and changes to Privacy Act protections covering the data of non-U.S. citizens held by the U.S. government. I will cover those two topics and also mention additional developments that have been happening in the last few months that I think are relevant to this committee.

On searches of electronic devices at the U.S. border, there is currently a regime of suspicionless searches. This means that the U.S. government claims the authority to search the electronic devices, including smartphones and laptops, of any traveller presenting themselves at the border, whether it's an airport or land, without any individualized suspicions and no requirement of a warrant or probable cause. This can include manual searches on the spot of the data and content on the devices, or it can include seizing devices and running them through what's called a forensic search, which is essentially a computer strip search where the government can access all files, including metadata and deleted files. In these circumstances, the traveller would be deprived of their device for days or maybe weeks.

This practice is currently the subject of litigation. It has been challenged by the American Civil Liberties Union, and the legal landscape is currently unclear. There are currently also pushes for greater transparency, meaning that the advocacy community in the United States, civil rights and civil liberties groups, are asking the government to release more information on whose data is being searched, what the nationalities of the people being searched are, and what the reasons for the searches are. At the moment, we only have aggregate data, and we know that, based on that aggregate data, the number of searches is increasing. In fiscal year 2016 there were about 19,000 device searches compared to about 8,500 in 2015. Again, we don't know why these numbers are increasing.

Turning to privacy protections, this is a separate issue not relating to travellers presenting themselves at the border per se, although it affects all data held by the U.S. government that would pertain to Canadians who are not citizens of the U.S. or are not green card holders or lawful permanent residents.

In January 2017, the administration issued an executive order stating that the Privacy Act protections would be stripped from all non-U.S. citizens and green card holders, meaning that all information held in U.S. government databases or systems of records would no longer be subject to the statutory protections that include protections on accessing the information that is held on you, correcting that information, and restricting the dissemination of that information beyond current enumerated exceptions.

Under the Privacy Act, for example, U.S. citizens have protections against their data being shared non-consensually. While there are exceptions for sharing data for law enforcement purposes and other enumerated exceptions, for the most part, individuals have to consent to their data being shared. Now with the new policy that says these protections will not be given to non-citizens, the only backstop is what are now known as privacy principles, and these fair information practice principles will be applied to the data of non-citizens and non-green card holders. While these are based on information privacy principles that have been the basis of many other worldwide privacy regimes, including the OECD privacy principles, nonetheless they do not provide the same protections as the Privacy Act. At this point in time, it seems fairly clear that non-citizens who have data of theirs held by the U.S. government do not have rights under the Privacy Act or any other statutory regimes to correct information that is held on them.

● (0950)

They may be able to use the Freedom of Information Act to request the information that is held on them by the U.S. government. That would be subject to any exemptions that the government could invoke to withhold information. Even if Canadians, for example, were able to get their information through a Freedom of Information Act request, there's now no right to correct that information, and there's no statutory right to limit the dissemination of that information for any reason that the government sees fit.

Those are the two main areas that I addressed in my previous testimony, and I will simply add that there is also currently an ongoing debate regarding retention of information on social media handles or social media activities of visitors to the United States. The government issued a notice on September 18, 2017, which made clear that it is retaining certain social media information that people provide in the course of applying for immigration benefits, which would include potentially information that visitors to the U.S. provide at the border. This information is being retained, and as of now it's unclear what the scope of that information being gathered is and how long it's being retained and for what purposes.

We do know that the default retention for this kind of information collected from visitors or others who are seeking immigration benefits in the U.S. is 75 years. As far as we can tell, there is currently a collection of the type of information on social media activity that's being done and being retained. The American Civil Liberties Union and other civil rights and civil liberties groups have been writing comments to the government highlighting the concerns that this poses for human rights and particularly for freedom of expression and freedom of association if travellers and visitors to the United States are fearful that they will be asked questions about their special media activity, and that the answers will be retained for a long period of time and potentially subject to being shared with other government agencies.

Thank you very much.

● (0955)

The Chair: Thank you.

Mr. Wong.

Mr. Solomon Wong (Executive Board Member, Canadian/American Border Trade Alliance): Thank you very much to the chair for the opportunity to present remarks on Bill C-21, which we believe is a fundamental cornerstone to the automated and more efficient way borders are managed for Canada.

As you mentioned, I'm an executive board member of the Canadian/American Border Trade Alliance. It's a group that has celebrated its 25th anniversary this year as a binational grassroots organization representing a number of public and private sector organizations. They're involved in Canadian and American trade, border crossing, transportation, tourism, airports, and bridge operators, among others.

As a voluntary board member for Can/Am BTA, I should also add that I have professionally worked for 20 years in all forms of border management between the U.S. and Canada, with my firm InterVISTAS consulting, specializing in different kinds of movements. Some members of the committee have seen my past work as the independent reviewer of the current pre-clearance act that was tabled in the House of Commons. I've also looked at the root causes of border delay, and that pertains to both goods movement and people movements.

The Canadian/American Border Trade Alliance is in full support of the provisions of Bill C-21, in terms of being able to have exit information that is recorded when individuals leave the country. As many have already testified before this committee, the intent of being able to expand the current capabilities that have been deployed since 2013 to provide information on Canadian citizens to support a range of different objectives on a restricted basis is that this biographic information on Canadians is going to be important to be able to close the loop in terms of the set of entries and exits from Canada. As we have seen in reports from the operating agencies, some 20 million records have already been looked at so far.

In granting new powers to government to be able to perform these kinds of activities, we always look at this in three ways. First, will this capability provide the ability for governments to better manage our borders, particularly the perimeter around the U.S. and Canada? Second, are there opportunities for efficiencies to be created to allow folks working for CBSA and IRCC to do more with what they currently have as resources? Third, from the Can/Am Border Trade Alliance perspective, are there opportunities to facilitate trade and travel?

Growth is continuing, particularly for international visitors and air travel, over 5% per annum over the next 20 years, as forecasted. In terms of being able to provide the capability for Canada to take the recommendations of groups such as ICAO, the International Civil Aviation Organization, in terms of recommended practices, certainly these are opportunities that are available for the Government of Canada to pursue facilitated efficiencies.

Imagine the age-old question that you face when you cross the border as to how long you have been away, and the amount of work to manually swipe passports and look at that particular question, and converting that to more productive types of questions, to be able to look at the kinds of people going across the borders.

As mentioned by other witnesses to the committee, Canada is not the first country to look at this. There are lessons to be learned from other countries that have sought to implement exit immigration data. I'll cite a couple of them.

In addition to the United States, recently the United Kingdom implemented the border systems program, which took effect in mid-2015. That represented a 20-year shift in the U.K. in terms of the way exit information is looked at. Prior to 1994, that was done through an exit booth when leaving the U.K. On departure, you would actually see an immigration person. As in a number of countries around the world, that was the mechanism. However, over the period of time of automating that capability and into mid-2015, the U.K. Home Office worked very closely with different port operators and airlines to be able to implement this. It very well might be a model to look at the provisions of implementing exit and entry from the Beyond the Border action plan. The issues were fairly limited.

● (1000)

Contrasting this was the move this past summer in the EU in putting forward a set of regulations in response to a number of attacks, in Paris and Brussels namely, and being able to have states in the Schengen area required to provide tracking of entry and exit information. In this case, the deployment was horrible by all accounts. Between May and June 2017, the number of delays was 97% greater than in 2016. In a number of countries, France and Spain namely, the delays in border formalities in August 2017 could reach up to two hours.

That is not the model to pursue because the ability to systematically and cohesively deploy this, as we have seen since the 2013 decision to provide a test of exit data, is certainly something that we've seen here in the experience to date. Granted, scaling this upwards is a different challenge, and certainly we're confident the agencies looking at this will have the ability to keep an eye on the ball to make sure delays aren't in place.

Interestingly, the world leader in this area, Australia, pioneered the approaches in the 1990s for advanced passenger processing. One of the first countries to fully automate the data in looking at arrivals, in April 2016, Australia moved ahead with what they called outward advanced passenger processing. This itself provided a similar capability to be able to have exit data put in place. Based on a long history of working collaboratively with the airlines toward implementation, that went fairly smoothly. I will also add that in my earlier remarks about finding facilitation benefits, Australia has a broader vision into the future. Its 2015 seamless traveller initiative has as its viewpoint being able to facilitate over 90% of travellers without stopping at a booth.

At Can/Am BTA we look at these examples and we applaud this. Where do we go from here? We would suggest three things to this committee to be looked at.

Number one is making sure that the border technologies being deployed are compatible with the powers that are provided in C-21. Although C-21 is limited to documents for outbound international travel or data coming in from CBP, we see a number of countries like Australia and the United States moving very rapidly toward biometric entry systems in addition to exit. While that's not the scope of C-21, it is certainly a progression and future that needs to be evaluated.

Number two, the passports that Canada uses do not have that ability for quick reading. Namely, the advantages of secure vicinity RFID is a technology available at a number of border crossings and that needs to be expanded greatly into the document itself.

Number three, and I can expand on this during questions from the committee, while ensuring that privacy is protected in terms of data, there are opportunities with the new Canadian centre on transportation data to be able to look at what this data source could help with on an anonymized basis. I reside in Vancouver, where there is a growing Vancouver-Victoria-Seattle tourism triangle. The ability to understand exits and departures much like cruise ships from Halifax and leaving by air for the United States, that source of information is currently a bit grey. There are opportunities other than this one that could provide advantages to both industry and government to understand those patterns of travel.

I look forward to questions from the committee.

● (1005)

The Chair: Thank you, Mr. Wong and Ms. Bhandari.

Ms. Damoff, you have seven minutes, please.

Ms. Pam Damoff: Thank you to both our witnesses for being here today and providing testimony.

Ms. Bhandari, you spoke a lot about social media information at the border. I wanted to clarify that our legislation that we're looking at right now does not deal with social media. Obviously we don't have the ability to amend U.S. legislation. I want to clarify that we're strictly looking at a page on our passport with biographical information. I think you probably were aware of that. Was that more for information purposes?

Ms. Esha Bhandari: That was for informational purposes, but also to just inform the committee that if there's any scope for recording the answers to questions that are given on exit, this might be relevant to limiting the scope of questions that would be retained.

Ms. Pam Damoff: As you probably know, our government puts a lot of importance on ensuring the safety and security of our citizens while also preserving their fundamental rights, which are protected in our human rights legislation, including the Charter of Rights and Freedoms.

We recently had the Canadian Civil Liberties Association testify. These are their recommendations:

> [It would be appropriate to include] an amendment to add a preamble similar to that...in the recent national security legislation, Bill C-59, and similar to that...in section 3 of the Immigration and Refugee Protection Act...both of [which] 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.

All of our legislation obviously is governed by the charter. Do you see a benefit to adding a preamble to this legislation, as per their suggestion?

Ms. Esha Bhandari: I want to clarify that as a representative of the ACLU, I'm not taking a position on Bill C-21 itself. I hope my testimony is helpful to the committee, but I don't feel qualified to opine on either the bill as a whole or particular amendments.

The question goes to the risk of racial profiling or other types of profiling in the enforcement of the bill. My understanding is that this involves information sharing as well, meaning that information collected by Customs and Border Protection on the U.S. side would be shared with the Canadian government and vice versa. It is relevant, again, to consider whether, if information is being collected on the U.S. side of the border, including responses to questions from travellers who are exiting, there is a risk of racial profiling.

Ms. Pam Damoff: It doesn't fall within our ability to regulate what happens in the U.S., or any legislation in the U.S., right? Sorry to cut you off, but my time is limited.

I'm going to turn to Mr. Wong for a moment.

Could you explain to us how the provisions of this bill would enhance cross-border trade and business between Canada and the U.S.?

Mr. Solomon Wong: Primarily, in looking at the powers themselves, in and of itself it's a cornerstone. How CBSA and to some extent IRCC choose to implement and use the provisions is where there are opportunities for facilitation. In the example I cited earlier, when Canadian citizens are coming back into the country and are asked how long they have been away, even though that's seconds in terms of the interaction, the ability to speed that up could create efficiencies in terms of the interaction between a CBSA border service officer and somebody coming into the country.

It would also give more opportunities to deal with potential issues as opposed to day-to-day questions of how long you have been away, which are really rooted in what we have had in the past in terms of the duties and taxes paid on goods. Since the limits have been elevated so much in successive governments, that really isn't as high a priority. Being able to find those kinds of things that could improve the process is what we see as the opportunity in Bill C-21.

● (1010)

Ms. Pam Damoff: I'm going to give the remaining time I have to my colleague Mr. Fragiskatos.

Mr. Peter Fragiskatos: Thank you to both of you for testifying.

Implicit, Ms. Bhandari, in your presentation is the idea that Canadians should be concerned about their electronic media being seized at the border upon entering the United States.

I've read articles that you have put forward with colleagues, citing figures about the amount of electronic media that is being seized. But even in 2016 when there was a significant increase in the number of electronic media that was searched by U.S. border officials, this still amounted to a very miniscule number. In fact, it amounted to less than 1/100th of 1% of all international arrivals, or 0.0061% of total arrivals to the United States had their electronic media searched.

If we look at the Canadian figures on that—and I don't have them—it's a much smaller number than 0.0061%. I think it's important to put things into context, but I do want to give you an opportunity to reply to that because I don't think it's an insignificant issue. You raise a legitimate concern, although it doesn't relate to the substance of Bill C-21. It's something we should be aware of, but we're talking about a very small number of seizures here.

Ms. Esha Bhandari: That's correct. We certainly know that percentage-wise it's a very small percentage of travellers who at the moment have their devices seized.

I think there are two concerns that animate our position. One, of course, is the domestic constitutional concern, which is not relevant to the committee in the same way. The other is a risk of selective searches. For example, we have seen cases of racial or religious profiling in the people who are singled out for device searches. We've also had at least one incident of a Canadian journalist, for example, being singled out at the border, and certainly press freedom associations here, and their counterparts in other countries, are concerned about the freedom to travel of journalists and others.

The concern even with the small percentage is that even when there's no protection or limitation, the searches can target individuals on impermissible bases, and that can really have an effect on freedom of movement and freedom of speech.

The Chair: Thank you, Ms. Damoff and Mr. Fragiskatos.

Just to remind both members and witnesses that questions and answers are to be directed through the chair.

I know Mr. Motz knows that perfectly well. You have seven minutes, please.

Mr. Glen Motz: Thank you, Mr. Chair, and to the witnesses for testifying today.

Through the chair, I will go to Mr. Wong first.

In a letter to several ministers in the spring of this year, the Canadian/American Border Trade Alliance and other business groups highlighted some areas of concern, one being the staffing shortfalls at the border crossing in the ports.

We've heard from witnesses in lead-up to today on this bill that, of course, we know this bill will include some new tasks for CBSA to carry out, and further resources will need to be allocated to CBSA in order to play out all of the requirements of this bill and to ensure that there's continued operation and smooth transition of both people and goods back and forth.

Apart from the potential border thickening that we've heard about, are there any other concerns you would like to highlight on the part of the businesses you represent regarding the continued free flow of goods back and forth between Canada and the U.S. once this bill takes effect?

● (1015)

Mr. Solomon Wong: I think very much, Mr. Chair, in terms of looking at opportunities for resourcing as well as what it is that border agencies as well as government as a whole need to be able to deal with big data.... This is, in essence, a large dataset that requires specified skills to be able to analyze, disseminate, as well as potentially act upon. On the kinds of interactions needed, I think numbers are one thing, but the skill set to be able to avoid false positives, meaning errant analysis of information, as well as potentially looking at ways to speed up the process are some things that would be looked at operationally as far as being able to get to the benefits of having powers under Bill C-21 is concerned.

Mr. Glen Motz: In addition to that, then, obviously you and your group would be in favour of investments at ports and border crossings, better hours—so expansion of CBSA times, because not all border crossings are 24-7 in Canada—and the use of new technologies to leverage this bill most appropriately.

Mr. Solomon Wong: Yes. Through the chair, that is something we would like to see in addition to a level of service that is easily understood in terms of trade. That goes to everything from wait times going across an airport, port, or land border to being able to make sure that, as our businesses become more 24-7, 365, there are ways to get to more services and availability.

Mr. Glen Motz: Thank you.

I will now direct a couple of questions to you, Ms. Bhandari.

Recently there was a failed U.S. refugee able to enter Canada and later carry out a terrorism-related act in Edmonton on a police officer as well as on some innocent civilian bystanders. Would you see any issue with Canada requesting information from the U.S. about other refugee applicants who cross the border?

Ms. Esha Bhandari: I'm sorry, could you clarify something? Requesting information as part of a law enforcement activity—is that the question?

Mr. Glen Motz: I mean a law enforcement activity or obviously, CBSA, border security, or national security interests.

Ms. Esha Bhandari: I'm not qualified to speak about the information sharing arrangements that the Canadian government has with the U.S. government, so I can't speak to what the bounds of those information sharing agreements are.

Mr. Glen Motz: Fair enough.

The CCLA and your organization have stated that there needs to be a limited time for which information is kept. However, when we need to retroactively look back on a case such as the Edmonton incident, having more information helps investigators piece together travel plans, potentially identifying similar plans, or potential acts elsewhere. Would you see it as a reasonable limitation to keep information with some strict timelines around how it's accessed and by whom?

Ms. Esha Bhandari: I can speak to that. As I mentioned, I think the default currently is 75 years for information retained by the U.S. government. I think that does raise privacy concerns when travel histories and travel information of individuals is retained for such a long period of time. Certainly it then becomes open and available in a way that information would never previously have been available to law enforcement or any other agencies. These have privacy concerns, and I don't think that the idea of limiting retention beyond the current default of 75 years wouldn't adequately outweigh law enforcement concerns. I think the overarching concern that groups such as the CCLA and the ACLU have is that this long-term retention of biographical information and all kinds of data represents a database that is vulnerable to both dissemination and use, and that really its existence can lead to privacy harms.

● (1020)

Mr. Glen Motz: Is it possible to achieve the same goals with limits on access rather than on retention?

Ms. Esha Bhandari: I think limits on access are an important tool. I think they don't fully address the retention question, because, as I mentioned, there can be privacy harms when data and information about individuals is retained essentially indefinitely for potential future law enforcement needs decades down the road. But I think limits on access are crucial, and particularly any limit that the Canadian government might negotiate with the U.S. government with regard to how information is shared within the U.S. government or even shared outside of government agencies, so with members of the public, for example.

The Chair: Mr. Dubé, go ahead for seven minutes, please.

Mr. Matthew Dubé: Thank you, Chair.

Ms. Bhandari, I want to go back to the retention thing, but just before that, I want to look at.... I was looking at the DHS report on phase 3 of the entry-exit border agreement, the Beyond the Border agreement, from last fall if I'm not mistaken, 2016. There is a part in here talking about privacy risk and mitigation which says, “CBSA permits CBP to use CBSA land border crossing data for: immigration management; law enforcement; national security; counterterrorism; public health and safety; and to the extent required by U.S. law”.

I'm wondering if you can speak to the concerns associated with having such a broad, open potential use of Canadians' data that we have agreed to share in this way, in relation to some of the privacy protections you were speaking about, because despite what I seem to be hearing from colleagues, there is an agreement in place to share that information, as you can tell from that excerpt of the DHS report.

Ms. Esha Bhandari: I think it needs to be credited as relevant to the committee. I would just note, Mr. Chair, that the Privacy Act protections that I mentioned, which have now been rescinded from data involving non-U.S. citizens, or non-green card holders, I think leaves it as an open question as to what the limits are on sharing of information pertaining to Canadian citizens.

As mentioned through the information sharing agreement, I think it is not clear whether there are any limitations on how that information shared with the U.S. government will in turn be protected by the U.S. government, and whether it can be shared across U.S. government agencies and to the public, or shared with other countries.

The default protection for a U.S. citizen is the Privacy Act. In the absence of the Privacy Act, there are not necessarily clear protocols and it might even vary from agency to agency in the United States.

Mr. Matthew Dubé: Thank you.

I will just go back to the idea of retention, and you already alluded to this in terms of future law enforcement needs. There is the 75-year period, which, let's face it, is, essentially as optimistic as we may be, someone's lifetime. But then in the same report on the same issue of entry-exit information, which is the bill before us, we see that any IIS, Internet information services, records that are linked to active law enforcement lookout records, CBP enforcement activities, or investigations will remain accessible for the life of the law enforcement activities to which they are related.

In the context of, for example, any kind of racial profiling happening at the border, which arguably could fall under CBP enforcement activities and things of that nature, are you concerned with that openness to the retention of data on someone in that particular context? Because, let's face it, any time there is profiling going on those categories could be used as justification for some kind of ongoing activity, or even with false positives as another example.

Ms. Esha Bhandari: There is certainly a risk of false positives and there is also a risk of disproportionate data retention, meaning that if there aren't safeguards against racial profiling on either side of the border with information that is then collected and shared between both countries, there is the concern that the databases of information skew disproportionately on the basis of those who have been profiled. That, again, contributes to the unequal treatment of individuals' privacy rights and data if some subset of travellers are more likely to have their information shared and retained. That is certainly a concern.

● (1025)

Mr. Matthew Dubé: There are colleagues reading more excerpts, but there is a sense that you get, reading through this report, that there are a lot of letters of intent and memorandums of understanding, and so forth.

Does your organization, with regard to how people are treated on both sides of the border, have concern about the extent to which many of these aspects of the agreement—length of retention, types of data retained, and the way in which it's shared—are relying on essentially, not to be too crass about it, a piece of paper, and not actually having any kind of legal force?

Ms. Esha Bhandari: I think that such agreements can be one tool if they are in fact enforced.

As an example, when the executive order on Privacy Act protection being removed from non-citizens was passed, the ACLU sent a letter to the European Parliament and the European Commission letting them know that U.S. assurances under pending agreements with the EU may be called into question now because those agreements that permitted data sharing between the EU and the U.S. relied on certain protections and guarantees of how information would be retained, and limiting access and limiting its use.

Certainly we think that if those agreements exist, they should be enforced, and particularly if those agreements form the basis for the information sharing.

Mr. Matthew Dubé: Great. Thank you very much.

I just want to end with you, Mr. Wong. I have a question.

You mentioned false positives. Are there concerns from any members of your organization, given that this information is going to be shared through different government departments to enforce different programs, of having folks who perhaps regularly cross the border, with whom I'm sure you work on many occasions, flagged erroneously by this kind of program, as different departments attempt to crack down on the use of different government programs, for example?

Mr. Solomon Wong: Mr. Chair, I don't think there are any direct concerns around how prescribed uses of data would provide tools to make the border more secure and efficient.

But in the implementation of name matches, I think there is a lot more attention that needs to be paid in terms of the mechanisms for recourse and other things that other witnesses have raised. This does become important from both an efficiency standpoint in terms of just making sure you don't have a lot of people who are stuck in secondary...which is the additional process for more scrutiny—

Mr. Matthew Dubé: I don't mean to cut you off, but I'm on my last 10 seconds. Would it be appropriate for the recourse to take place directly vis-à-vis CBSA?

Mr. Solomon Wong: Can/Am BTA doesn't have a stated position on that topic itself, but my personal view is that it is inherently complex to find your way to the part of the Government of Canada where you would get a recourse mechanism. Passenger protect has its own. You have different channels, and there's certainly room to make that simpler.

The Chair: Thank you, Mr. Dubé.

Monsieur Picard, you have seven minutes, please.

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

Mr. Wong, I would like to hear from you on the trade side of things. Do I understand correctly that you think Bill C-21 should be one of many tools to increase and facilitate trade between the two countries and to do so in a more efficient way?

Mr. Solomon Wong: We do see provisions, Mr. Chair, that provide additional powers related to outbound inspections. Certainly from the use of the powers, we'll have to see what that means in practice. We have seen the responses from CBSA to the committee on some of the questions on that, but it's something that, again, will depend on how things are exercised in practice.

The U.S. and Canada largely have co-operated a lot in terms of data elements and different things already, in terms of manifest information on shipments. Certainly the approach and moving towards other initiatives unrelated to Bill C-21 around single window and those kinds of things are still very important, but they are outside of the relevance of this particular piece of legislation.

Mr. Michel Picard: In terms of the proposed changes to subsection 95(1) in part V of the Customs Act, besides the transit issue, it has been suggested that from now on people would have to declare everything to customs, every bit and piece of information—contents, goods, whatever—before leaving the country. In fact, exportation in part V of the Customs Act is much more elaborate than just section 95, and people are not supposed to declare everything, except what is regulated.

Is it your understanding that the changes that are suggested in the new section 95 will change that, or is it just a matter of precision with respect to transit and answering the customs officer if someone asks you a question?

● (1030)

Mr. Solomon Wong: Our understanding of the use of that section is that it's a power that's available for additional questions, just as there are separate provisions already dealing with currency. The expansion under Bill C-21 as proposed would allow for an officer, a BSO, if they do need to ask somebody a question about goods in their possession that may be controlled exports, to be able to answer truthfully.

Mr. Michel Picard: It's pretty much business as usual with an exception where required. A customs officer may act on specific cases.

Mr. Solomon Wong: That's our understanding in terms of the enforcement power that's provided for questions and a potential investigation.

Mr. Michel Picard: Thank you.

Ms. Bhandari, if I go into the U.S., my phone and computer may be searched, and all the content in it may be looked at, and I can't do anything about that. Is that what you said?

Ms. Esha Bhandari: If it's just a visitor, not someone who has a lawful permanent resident status in the United States, then individuals who don't consent to have their devices searched or who don't consent to answer all questions may be turned away.

Mr. Michel Picard: Does that also apply to the professionals who are going to work in the U.S. for a few days or a few weeks? Are they subject to a search?

Ms. Esha Bhandari: Yes, all visitors, regardless of the length of time, are subject to search.

Mr. Michel Picard: What if that happened the other way around? If a U.S. citizen's iPhone and computer are searched by a foreign government, does he have any recourse? Does he have any tools, any way to go against that or prevent it? How does the U.S. treat its own citizens in a similar case the other way around?

Ms. Esha Bhandari: To my knowledge there isn't any legal recourse, at least not through the U.S. system, for American visitors travelling abroad.

One of the reasons we advocate for limitations on the U.S. government not only on device searches—which I understand are not an issue in the bill under consideration—but in terms of the questions asked and the information recorded, is that other governments may behave in a reciprocal manner. They might similarly demand information about people's activities and record, retain, and share that information in a way without limitations. Our concern is that if this becomes a worldwide norm, that will have implications for freedom of speech, freedom of association, human rights, and people's ability to travel freely without concern that their privacy will be unduly burdened.

Certainly there's a concern that whatever the U.S. government implements in terms of a policy of data retention will be copied by other governments, and that there will be limited recourse for people who face the choice of either travelling or not.

Mr. Michel Picard: What about the concern about the privacy side of it? My data will be gathered in a database, handled by CBSA or whatever customs power. There's nothing I can do against someone who decides to steal a database and sell it to someone. To a certain point there's a limit to my own security, regardless of the technology I use.

Ms. Esha Bhandari: That is certainly a reason, Mr. Chair, to think hard about the amount of information that is retained and collected in the first place. There are concerns about the security of data any time it exists, and any time it exists for a long period of time. Any time more information is collected than is strictly necessary for the government activity at issue, that is a concern.

Mr. Michel Picard: In other words, based on what Bill C-21 suggests, the fact that my information is already in my passport, information that I give to every country I visit is pretty much basic information with not that much impact. Is that right?

● (1035)

Ms. Esha Bhandari: My understanding is that if the bill were to lead to more complete databases, by which I mean both the U.S. and Canadian governments would have a complete picture of a traveller's entries and exits over time, that could certainly paint a very detailed picture of a person's life. That information existing for a lengthy period of time can pose privacy risks, both because of the risk of the information getting out—being stolen—and because it could be shared with other government agencies for whatever purpose it may be.

The Chair: Thank you, Mr. Picard.

Ms. Gallant, you have five minutes, please.

Mrs. Cheryl Gallant: Thank you, Mr. Chairman, and through you to the witness, with the crossing of goods do you see the ability for data on Canada-U.S. exits to be cross-referenced in almost real time? For example, you could have a truck crossing the border at Thousand Islands, pulling in, dropping something off, and then doing a U-turn and coming back over. Will the border agents on the Canadian side know the answers to the questions that the trucker gave to the U.S. border agents going into the U.S.?

Mr. Solomon Wong: Through the chair, in terms of capabilities under Bill C-21, that particular scenario may be a little outside the scope of the bill. But the scenario you describe is a long-standing issue that has been documented about in-transit movements through the other country, so a Canada-to-Canada movement through the U. S., or a U.S.-to-U.S. movement through Canada.

In terms of what makes for a logistical flow, the ability to make that transit movement, which is basically a domestic movement through another country, as seamless as possible is important in making sure both CBP and CBSA have the right mechanisms to deal with that data.

Mrs. Cheryl Gallant: Where, if at all, do you see any vulnerabilities in bringing goods across the border? Where might they go undetected or might there be things on a manifest that are not matching what is actually in the back of the truck?

Mr. Solomon Wong: On the question on the integrity of the borders, there are mechanisms to make sure that the trusted trader programs are properly supported, such as the free and secure trade program, as well as the U.S. customs trade partnership against terrorism, and the Canadian partners in protection program. The more those kinds of programs are supported and expanded, the better that scenario will be addressed. We're dealing with the ability for supply chain security all the way back to the factory, if it's a manufactured good, through to the destination, rather than just the transaction at the border. By then it's too late.

Mrs. Cheryl Gallant: In terms of pre-clearance and exit information, are there any additional provisions you're aware of that should be put into place for radioactive substances?

Mr. Solomon Wong: I know there's been a lot of attention particularly with CBRN, chemical, biological, radiological, and nuclear, in terms of detection, but certainly the ability to install detection portals is one approach that has been taken. There have been tests on the Canadian side. CBP has wide deployments. At this stage that's as much detail as I have for this committee off the top of my head.

Mrs. Cheryl Gallant: In terms of exits, some countries have an exit fee. In order to implement the system, do you see any fees as being required on the part of the people and companies actually crossing the border?

Mr. Solomon Wong: If I can clarify, are we talking about the air mode or other modes, or just in general?

● (1040)

Mrs. Cheryl Gallant: Other modes, like land.

Mr. Solomon Wong: Through the chair, it is our expectation in the deployment of this that there would be no fees added on a transaction or other basis to pay for any kind of data system. Based on the way that Bill C-21...and the implementation to date, and in terms of information sharing, the idea is to reduce duplication and reuse data that's already available: exiting Canada as the entry record to the U.S. and exiting the U.S. as the entry record to Canada. Those are the efficiencies that would be gained from that as opposed to a transactional fee.

The Chair: Thank you.

For the final five minutes on the evening of the commencement of the World Series, Mr. Spengemann is batting the cleanup.

Mr. Sven Spengemann: Mr. Chair, thank you very much.

Thank you, both, for being here today and providing your insights and expertise. I want to take the opportunity of your presence to ask a fairly general question for the benefit of the committee and the benefit of Canadians.

Both of you have professional engagements on both sides of the border. You understand Canada and the U.S. very well. Could you outline for the committee the differences that you see in the way that Canadians and Americans think about the issue of privacy? Feel free to be anecdotal in your answer or as general as you wish. I think it might be helpful for the committee to see if there are any fundamental differences in how the public reacts to privacy legislation, to the collection of data, all in the context of a very tight, intermeshed relationship on the leisure, education, and business side.

Ms. Bhandari, perhaps I could get you to start, and then I'd like to hear from Mr. Wong as well.

Ms. Esha Bhandari: Thank you.

Once again, I want to thank the committee for inviting me to testify.

I would urge you, Mr. Chair, simply to consider in any new policy or new information sharing agreement to not discount the very real privacy concerns, and in fact, simply to weigh them in the balance. I think travellers to the U.S. and travellers to Canada undoubtedly value their privacy. There's no doubt about that. I don't wish to undercount the importance of the trade and the travel between the two countries, and the necessity of making their profits easier for all, which I think is a benefit, but I do think it is important for the committee to simply consider the steps or the changes that can be made that would ensure that the privacy interests are adequately balanced. I think that people increasingly are aware of the existence of massive quantities of data on them that are held not only by governments but by private parties. We've seen a rise in people taking steps to protect their privacy, to minimize the data that they put out into the world. I don't think this is any less true of travellers between both countries, and I think that people are increasingly concerned about such things as hacking of information and hacking of databases, of which even governments are vulnerable. I would conclude simply with that: the privacy considerations should be weighed.

Mr. Sven Spengemann: Mr. Chair, perhaps I may interject there for a moment. Ms. Bhandari, in your work, have you run across any appreciable differences in the way that Canadians versus Americans act on privacy legislation?

Ms. Esha Bhandari: I have not run into any appreciable differences. I know there's currently a large debate happening in the United States very much focused on data privacy. I'm less familiar with how that debate has concretely taken place in Canada.

Mr. Sven Spengemann: Thanks very much.

Mr. Wong, how about you? Have you noticed any differences?

Mr. Solomon Wong: I have two points. Both countries are going through the same phenomenon in terms of the expectation of privacy from the public overall, particularly with the very same mechanisms we spoke about earlier in the committee. The social media mechanisms, the habits of publishing photographs, posts, anything in the public domain have certainly shifted the way privacy is perceived in both countries, and the expectation of privacy, I would argue, compared to a discussion like this 20 years ago, would be quite low.

Specific to both countries and the approach on topics like this, the IRCC testimony before this committee, Mr. Chair, homed in on a key term, that there has been an examination on using privacy by design. I know that just from the standpoint that at Can/Am BTA, we've had speakers present on privacy by design. It is encouraging that this is being looked at early on, in addition to the requirements of the privacy impact assessments that are required. In the previous administration, in October 2010, the privacy commissioners around the world all endorsed privacy by design as a new standard to aspire to in terms of developing programs. That is integral for the fidelity of any idea that uses big data going forward, because at the onset, there is thinking around the issues of retention, who has access, and those kinds of things built right into the development of systems, rather than simply the submission of an impact assessment.

● (1045)

The Chair: Thank you, Mr. Spengemann.

On behalf of the committee, I want to thank both Ms. Bhandari and Mr. Wong for their contributions.

I just remind colleagues that we will be going to clause-by-clause consideration next Thursday morning at this time, and if there are amendments, to submit those amendments by five o'clock this afternoon.

There will also be a subcommittee meeting where we'll be organizing for the indigenous corrections study. For those who want to get witnesses in, my preference would be that we do it through the subcommittee so that we can organize efficient hearings starting a week from today.

Again, thank you.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: http://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : http://www.noscommunes.ca