House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 010 • 3rd SESSION • 40th PARLIAMENT

EVIDENCE

Tuesday, April 27, 2010

Chair

Mr. Paul Szabo

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, April 27, 2010

● (1130)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): Order. This is the tenth meeting of the Standing Committee on Access to Information, Privacy and Ethics. Our order of the day, pursuant to Standing Order 81(4), is the main estimates for 2010-11, vote 45 under Justice, referred to the committee on Wednesday, March 3, 2010.

Our witnesses today from the Office of the Privacy Commissioner of Canada are: Ms. Jennifer Stoddart, Privacy Commissioner; Chantal Bernier, assistant privacy commissioner; Elizabeth Denham, assistant privacy commissioner; and Tom Pulcine, director general and chief financial officer, corporate services branch.

Welcome to all of you and to your other team members from the commission, Madam Commissioner. I understand that you have an opening statement for us with regard to your main estimates. I'd ask you to commence now.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chairman. We're happy to begin.

We're of course very grateful, once again, to be able to come before you to report on what we plan to do with the budget, which we hope you will vote for us in this present session.

I'd like to say first that I greatly appreciate the positive, productive relationship that my office has enjoyed with this committee over the years. I particularly appreciate the unwavering support you have shown for our goals, our initiatives, and our evolution. I will address all of these in short order.

First of all, I'll start with the question of human resources, which has often come up before this committee. As you know, Mr. Chair, my office has undergone a great deal of change over the past seven years, since I first appeared before a parliamentary committee.

Thanks to stable and appropriate funding from Parliament, we've been able to attract and retain the full complement of managers and employees needed to carry out our agenda. For example, we have hired and trained more than a dozen investigators to help us tackle a serious backlog of complaint files. We've also bolstered our in-house expertise in the all-important area of technology, with targeted hiring of some very knowledgeable people.

We have reached out to younger people so as to inject a level of energy and vibrancy into our organization. Some of these younger people are with us today. They are the next generation of privacy specialists.

I'd like to quickly go over some of our accomplishments in the last year.

Last week, as you may have noticed in the media, we joined data protection authorities from around the world in expressing deep concerns about Google and other global technology leaders for introducing new applications without due regard for the privacy norms and laws prevailing in our respective countries.

Last July, we published our findings into an investigation into the privacy policies and practices of Facebook, highlighting concerns about the company's transparency with respect to its use of personal information.

On the public sector side, we worked with the integrated security unit of the Vancouver Olympic and Paralympic Games to ensure that privacy rights were respected before, during, and after the Winter Olympic Games.

We also scrutinized the many new security measures affecting international travellers, particularly the full-body scanners now being rolled out at Canadian airports.

We, along with our provincial colleagues, alerted parliamentarians to the privacy concerns in legislation aimed at giving Canadian law enforcement, national security agencies, and others broader powers to acquire digital evidence to support their investigations.

Another topic that has come up frequently in this committee is the question of our backlog. We're very pleased about the recent resolution of a long-standing backlog of complaint investigation files older than a year.

The backlog problem had grown to unacceptable proportions in the past several years. With targeted funds that we received from Parliament in 2006, we were able to hire new investigators and appoint key people to streamline the intake function, and we re-engineered entire systems and processes.

The backlog has now been eliminated. Moreover, we have put in place new measures, such as an emphasis on early resolution of complaints, to ensure that we do not fall behind again.

With the complaints backlog out of the way, we can now focus on more systemic issues and better service to Canadians.

[*Translation*]

I will now move on to the four policy priorities. We can also reflect on the bigger picture: the current and emerging challenges to privacy, in this country and globally, and how our office can continue to make a difference in the lives of Canadians.

In that context, we continue to advance our work in the four policy issues that we anticipate will most dramatically affect privacy in the years ahead: national security, information technologies, genetic technologies and the integrity of people's identity.

We have been deepening our understanding of these important issues through comprehensive research, increased public education and participation in policy discussions with a wide range of experts and other stakeholders.

Over the past year, we have also been examining our other core activities to ensure we are serving Canadians in the most effective manner.

For instance, we are retooling our processes for auditing compliance with our two acts. We are also transforming the way we review privacy impact assessments so that our activities are guided more explicitly by analyses of risk and alignment with our identified priorities.

With an eye to better service delivery, we were also encouraged by Parliament's progress on ECPA, the Electronic Commerce Protection Act. While Industry Canada has the lead on this initiative, my office, the Competition Bureau and the CRTC will ultimately share an oversight role.

I know that Assistant Commissioner Elizabeth Denham appeared recently, accompanied by Tom Pulcine, to discuss the supplementary estimates attached to this initiative, and we appreciate your support of those estimates.

Thanks to amendments to PIPEDA embedded in the legislation, ECPA would give me the authority to be more selective in the investigations we pursue, thus enabling us to focus on more complex or systemic issues.

Another laudable aspect of ECPA is that it would deepen our capacity to share information with other data protection authorities, in Canada and abroad. Collaborative enforcement has become essential in this globalized world, where data flows unimpeded across borders. The need for collaborative enforcement was made clear with last week's joint initiative related to Google.

For these and other reasons, we sincerely hope this bill will be reinstated and passed during this parliamentary session.

● (1135)

[*English*]

To continue, I'll talk a bit about legislative reforms and alternatives.

We also look to this committee's support for other measures that would allow us to better deliver on our mandate. For instance, while we accept that amendments to the Privacy Act, which we have discussed intensively in this committee, are not moving forward at this time, we are implementing a range of administrative alternatives.

For example, we are helping to improve privacy training among public servants, encouraging data breach notification as the norm across government, and ensuring that all privacy impact assessments, called PIAs, embed an assessment of necessity, a bedrock principle of privacy protection.

To underline our impact in the latter area, I want to note that the number of PIAs submitted to us rose from 64 in 2008-09 to 102 in the past fiscal year. We've also been reaching out to departments and agencies, individually and through a very successful PIA workshop, to make sure they understand what we would expect a good PIA to include.

Meanwhile, under PIPEDA, we look forward to further amendments that would make breach notification mandatory, as a means of better protecting the personal information of Canadians.

I'd like to talk now about the consumer consultations we'll be holding in three major Canadian cities in the next few weeks.

PIPEDA, the private sector law, also enters another review period next year. To inform this process with a further understanding of key emerging issues with important impacts on privacy, we're about to launch a groundbreaking consumer consultation on the online monitoring, tracking, and profiling of consumers by business, and cloud computing technologies.

All the members of this committee were sent invitations to these consultations, which will also be webcast across Canada. The first one is on Thursday of this week, in Toronto, with Montreal following in May, and Calgary in early June.

We have been working very hard to expand our office's presence across Canada. A quick scan of our website will reveal a plethora of fact sheets, guidelines, videos, youth competitions, blogs, and other products. Also, you can now follow us on Twitter.

In an approach supported by Parliament, we are also expanding our presence in the regions. We have bolstered our presence in Atlantic Canada and increased our activities in Quebec and in the west.

We are also establishing a satellite office in Toronto. Like Parliamentarians and many of our stakeholders, we feel this is a sensible initiative since so many of the companies we regulate under PIPEDA are headquartered there. We will be making use of existing resources for this work, so we're not asking for additional resources from Parliament at this time.

In conclusion, I've touched on but a handful of our activities over the past year and our plans for the year ahead. I hope I've been able to show you how we're pursuing our corporate priorities, which you know about but which remain unchanged. I'll just remind you that they're about improving service to Canadians; helping individuals, organizations, and institutions make informed privacy decisions; advancing global privacy protection for Canadians; furthering our priority privacy issues; and strengthening our internal capacity so the office can continue to carry out its mission for many years to come.

Mr. Chair, I understand that in this session the members are also interested in the issue of video surveillance. We would be happy to answer their questions. We've brought some materials, such as our guidance on video surveillance for public and private sector organizations.

And of course, we would be happy to answer the questions you have, Mr. Chairman.

● (1140)

The Chair: Thank you very much, Commissioner, and thanks to your team, for obviously a very busy growth period.

We're certainly pleased to hear about the human resources stabilization. I don't have the actual numbers, but just to tidy this up, can we have your turnover information and current vacancies?

Ms. Jennifer Stoddart: Our projected unplanned turnover for the year is, I believe, 14%. I believe the honourable members do have some statistics on our office HR resources.

Of the departures last year, half of them were planned and half unplanned. The planned are people who retire; the other half is made up of students, term workers, and people who accept transfers and promotions elsewhere in the public service. At the present time, I believe we have six unstaffed positions of the 173 that have been accorded to us by Treasury Board.

The Chair: Thank you.

That tells me that the Privacy Commission is back in business.

Ms. Jennifer Stoddart: Yes.

The Chair: That's terrific.

Mr. Easter, please.

Hon. Wayne Easter (Malpeque, Lib.): Thank you, Mr. Chair.

Welcome, Commissioner and colleagues.

I will admit that I never, ever figured that the Privacy Commissioner would end up on Twitter.

Even I won't use Twitter; I might say something foolish, Pierre.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): That's impossible.

Voices: Oh, oh!

Ms. Jennifer Stoddart: Honourable member, we're not on Facebook—

An hon. member: [*Inaudible—Editor*]

Hon. Wayne Easter: No, that's true.

On your consumer consultations in your report, your remarks, this is an area that we hear a fair bit about, that for people using credit cards and everything else, there seems to be a profile established on individuals and then they're targeted for certain advertising and so on. Is that what you're talking about in these consumer consultations? Can you give me a little more information on that?

Ms. Jennifer Stoddart: Yes, we're talking about that in, I believe, two of the three consultations. I'm fortunate to have very talented and knowledgeable assistant commissioners who in fact are shouldering a lot of the day-to-day burdens.

Could I ask Assistant Commissioner Denham, who has organized these workshops, to give you more details?

Hon. Wayne Easter: Go ahead.

Ms. Elizabeth Denham (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): The consumer consultations in Toronto and Montreal are indeed focused on the kind of profiling and tracking that happens with online advertising. We're trying to understand how industry, technology, and the business models work.

We are trying to get from academia, industry, and consumers their views on the way personal information is collected and profiles are developed for advertising. We will produce a policy paper at the end of the consultations that will help us grapple with whether or not our laws are up to regulating the new technologies and the new online tracking.

● (1145)

Hon. Wayne Easter: Thank you.

In another area, we understand that you've done a number of investigations over the last year into privacy matters. Some investigations we're aware of; no doubt there are some that we're not. Can you list for us what those investigations are? Are you required them to make them public? What's the procedure there?

Ms. Jennifer Stoddart: We are required to keep confidential the details of the investigation, in fact, or the identity, shall I say, of the organizations and the people involved. We don't list every single investigation that we do. Some of them are repetitive; the fact situations are repetitive and so on.

We do make a resumé of the decisions that can be useful for the public, and particularly under PIPEDA, we have almost 400 decisions, I think. Sometimes you'll see the name of the respondent and the complainant, but that's very rare. They're listed on our website so that the public can better understand how we interpret the law. We have fewer decisions that we publish under the Privacy Act, but we're working on that so that, again, citizens know how we look at their complaints in relation to the federal government.

Hon. Wayne Easter: So it's just basically the general area and not the specifics that are reported?

Ms. Jennifer Stoddart: No. They're kind of what lawyers call case summaries. Often they can be a page and a half or two pages long. They explain what the complaint was, what the factors were that we looked at, and what the conclusion was.

Hon. Wayne Easter: Thank you.

As you're no doubt aware, this committee is currently examining the issue of allegations of political staff in a minister's office engaging in interference in information from government, both through access to information and through the process of legitimate enquiry. This has been in the public arena fairly substantially recently, especially as it relates to the PMO.

Have you had any concerns regarding the possible exceeding of the legitimate role of the federal government or personnel in regard to the Privacy Act and whether there are actual contraventions of the letter of the law or at least the spirit of the law?

Ms. Jennifer Stoddart: I believe, honourable member, that we did receive a complaint of that nature. The result of the complaint was that the allegation was not founded in terms of the law having been exceeded for political reasons, as I remember.

So I think it's always a concern. We don't have.... There was another case we investigated some years ago where a reporter alleged that his request to the Prime Minister's Office had been jeopardized by the fact that his identity was known. Our investigation revealed that, as I remember, the staff surmised from the type of request it was and that there was no evidence that the identify of this person had been revealed.

Hon. Wayne Easter: So in terms of those cases, we wouldn't have the specific case, but there would just be a summary of what you found. Is that correct?

Ms. Jennifer Stoddart: Yes.

Hon. Wayne Easter: In the ones you've mentioned?

Ms. Jennifer Stoddart: Yes, but the whole case goes to the parties involved. So if a complaint is made, then, a report is sent out to the complainant and to the respondent.

Hon. Wayne Easter: Okay. I guess we'll leave that. And at least the summaries are available on your website...?

Ms. Jennifer Stoddart: That is correct.

The Chair: Thank you.

If I may, just as the last question on it, on the information that's reported to either a complainant or the person or party against whom that complaint was made, are they held to any privacy standard or confidentiality standard?

Ms. Jennifer Stoddart: I don't think so, Mr. Chairman. I think that certainly the complainants may choose to make available the information that is in their report—if they so choose. We can't in a way that would identify the complainant, but the complainant may. I believe that if the federal government were a respondent, it would still be bound by its duty to keep personal information confidential.

● (1150)

The Chair: Understood.

Madame Freeman, s'il vous plaît.

[*Translation*]

Mrs. Carole Freeman (Châteauguay—Saint-Constant, BQ): Good morning, Ms. Stoddart, Ms. Bernier and Ms. Denham. Thank you for being here this morning.

I want to start by congratulating you and your team, Ms. Stoddart. I am very pleased with the job you have done. On Saturday, I was reading the paper and learned that you were leading the way in terms of the social networking site Google Buzz, as you did with Facebook. Given the tools at your disposal, the manner in which you work, as well as your relationships with privacy commissioners around the world, whether in New Zealand, the Netherlands, the United Kingdom, France, Ireland or Germany, I would say you are doing a fine job and have an outstanding team.

My question has to do with your priority issues this year. You identified four, which you mentioned earlier: information technologies, national security, the integrity and protection of people's identity and genetic technologies. Clearly, given the vast number of areas in your field of expertise—and given all the new technologies—you chose four out of a slew of others, I would imagine.

What criteria did you base your choices on?

Ms. Jennifer Stoddart: Those choices were determined two or three years ago, I believe. We consulted with staff members whose job it was to stay abreast of privacy developments. We chose these four priorities because, strategically speaking, we felt they were the areas most likely to affect the lives and privacy of Canadians in the years ahead.

I will ask Assistant Privacy Commissioner Bernier to elaborate further. In fact, it is easy to choose the areas, but much harder to stay on top of them, to continue to make choices and to accomplish objectives.

Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): What we did was set up four task forces to really focus our efforts on the four priorities, which, as the commissioner said, were chosen for their relevance and because they represent the biggest risks to privacy today.

The national security task force worked hard and made significant strides in a number of areas, in terms of expanding our knowledge and understanding of the issues, and forging stronger ties with national security and law enforcement agencies to ensure we really understood everything involved. Internally, we also carried out more in-depth analyses. We focused on analyses addressing all aspects of national security, including the FINTRAC audit. You will recall that the audit was published recently. Our analysis of former Bills C-46 and C-47 is another example.

We organized workshops to discuss the issues surrounding genetic technologies. It is an area where a lot is still unknown. We did so of our own accord and in cooperation with Genome Canada. In terms of information technology, there again, we strengthened our capacity by engaging experts and keeping a very close eye on all technological developments.

Lastly, in terms of identity integrity, most of our focus was on public education and youth outreach, in order to ensure that Canadians are able to protect themselves against identity theft.

● (1155)

Mrs. Carole Freeman: If I understand correctly, work on your priority issues is already under way. The committees are working very well, and they will produce findings concerning the four priority issues. Do you plan to submit a final report? What do you plan to do exactly?

Ms. Chantal Bernier: Each task force has a matrix of success factors, so deliverables. It depends on the issue. In genetics, for example, the workshops that we organized and contributed to will allow us to review one of our outdated documents in order to take stock of the latest developments in genetics and privacy. The same goes for security.

Mrs. Carole Freeman: Give me some examples, then.

Ms. Chantal Bernier: Our participation—

Mrs. Carole Freeman: Obviously, you are talking about three years. Things happen so quickly, you have to keep up-to-date.

Ms. Chantal Bernier: Indeed.

We recently met with the Assisted Human Reproduction Agency of Canada, which is exploring a whole new realm of possibilities in terms of protecting genetic information. We are part of that. I represent the commission on the National DNA Data Bank Advisory Committee, where all kinds of methods for implementing the legislation, using DNA, are posing challenges to privacy.

Mrs. Carole Freeman: Those are very worthwhile issues.

You work with the department responsible for national security. Can you tell us what specific areas you are working on right now?

Ms. Chantal Bernier: We worked with department staff to gain a deeper understanding of the context. It is critical that we understand the challenges and issues they face, but we challenge them, as well.

Mrs. Carole Freeman: Yes, can you describe the challenges? When I was on the justice committee, I had the opportunity to ask people questions, and it was quite difficult to get information out of them. Oh, oh!

Ms. Chantal Bernier: Yes. For instance, the first step in our analysis of former Bills C-46 and C-47 was to sit down with them and ask them to justify the powers conferred to them under the bills. So numerous meetings were held, experts who were no longer necessarily at the agencies—so who had a certain perspective—performed an analysis and people in academia were consulted.

We formed our own opinion, we did our own analysis of the bill, and we wrote to the chair of the Standing Committee on Public Safety and National Security. And we sent a copy of that letter to the chair of your committee. In the letter, we raised some real questions about the two bills.

Mrs. Carole Freeman: What kind of cooperation did you get from national security....

Okay, then.

[*English*]

The Chair: We'll find out in the next round.

Mr. Siksay, please.

Mr. Bill Siksay (Burnaby—Douglas, NDP): Thank you, Chair.

Thank you for being here again, Commissioner, with your colleagues.

Commissioner, I, too, want to congratulate you on the initiative around the Google Buzz issue. Is that kind of international cooperation a personal initiative that you take or is there an international body of other privacy protection officers? How does something like that come about?

Ms. Jennifer Stoddart: Thank you for that question, because it's important to situate what happened in the context.

There's an international privacy commissioners' conference. That has existed for about 25 years now. Increasingly within that conference we're coming to the realization that the issue is common action, common standards, and common enforcement goals, particularly when faced with the rise of global business, which has been dramatic in the last 10 years, and then the rise of the new social online media, which have been around for only two or three years.

We've done quite a few things over the years with this group. Last year, we were working on global standards to try to bring standards across different countries closer together, because global business says that it doesn't know what the standard is: that it's this in one country, while the procedures are that in another country. So we're trying to facilitate the understanding of privacy.

It's within that context, and more particularly within the context of the work at the OECD, where Canada, through the presence of the delegation led by Industry Canada, plays a significant role in OECD privacy and security workshops. Some of us were there in Paris on that occasion, and that's when the idea of a common position on this particular issue arose.

Mr. Bill Siksay: Is the OECD the key international body that looks at these possibilities of cooperation around international enforcement issues?

● (1200)

Ms. Jennifer Stoddart: I'd say yes, it is the most formally constituted body. The commissioners don't have a secretariat, and the conference changes from one year to the other. In fact, the OECD was the organization that defined the information principles in 1981. That's the basis, I think, not only for our Privacy Act, but also for PIPEDA and many other countries' standards.

Mr. Bill Siksay: Has Canada taken any particular initiatives around cooperation and international enforcement, globalized enforcement, on these kinds of privacy issues that emerge?

Ms. Jennifer Stoddart: Yes. A couple of years ago we were very active with our colleagues, particularly in the Federal Trade Commission in the United States, as well as with some other European countries, in setting up a transborder complaint-sharing mechanism.

For example, if I get a complaint about a New Zealand company operating in Canada, I can ask my New Zealand commissioner for help. That person doesn't have to, but it's a kind of way of structuring requests for assistance across the OECD members.

Mr. Bill Siksay: That's great.

Moving onto something else, I was actually going to ask about the electronic commerce protection legislation, because you said that would increase your mandate around some of these issues. Can you say a little bit about what the change would be and where you would find the mandate? And do you need more funds? Is this an emerging area that requires more of your office?

Ms. Jennifer Stoddart: ECPA, the Electronic Commerce Protection Act, although it is basically an anti-spam legislation, which is long overdue, also has some clauses included in it that I have asked for and the government agrees would be.... I think there's wide agreement that they would help me become more efficient.

One is discretion to not have to take all the complaints, so that we could pick and choose and look at the more systemic issues. The other one is to be able to more fully share information, including, if necessary, details of complaints with other provinces and territories in Canada and internationally as may be needed for enforcement.

There is an envelope for the eventual enforcement of ECPA, which would be led by Industry Canada. We were here about three weeks ago on that. From memory, I think it's first four person-years and then six person-years and $200,000 recurring. If ECPA comes in, you will see that it's added on to our money that you will vote under the main estimates.

Mr. Bill Siksay: On the cooperation with other international privacy protection agencies, that's in your budget. Is that an emerging area? Is more of that happening recently? In terms of the money you get to do your job, is that covered?

Ms. Jennifer Stoddart: Yes. I think that's covered substantially now. We're not asking for any new funds. Of course, we try to make use of new technologies, and our staff e-mail, talk, and so on, so it doesn't necessarily take any more personal travel in that sense. It's more a mutual realization that we have to get together to send strong messages to global businesses.

Mr. Bill Siksay: What will happen to the staff who were brought on board to deal with the backlog? Now that there's no backlog, I guess there's probably not as much work, specifically the kind of work that they were doing in the past. What will they be doing in the future?

Ms. Jennifer Stoddart: Yes. Well, we didn't bring in extra staff over our complement to deal with the backlog. We used some former employees on contracts, some consultants, and some lawyers who had knowledge in the area. So there will be no job loss for permanent staff. Indeed, I feel very strongly about preventing job loss for permanent staff.

Mr. Bill Siksay: You mentioned bolstering your regional presence. Can you expand on that a little? What's it going to look like in the various regions?

You specifically mentioned Toronto in terms of a satellite office. Can you tell us the percentage of businesses under PIPEDA that are based in Toronto? You mentioned that was why you had chosen to do this.

What will the regional structure look like and what are the changes?

Ms. Jennifer Stoddart: It has been delegated to Assistant Commissioner Denham. Could she answer that question, please?

Ms. Elizabeth Denham: Thank you.

We've looked at the percentages of respondents under our private sector legislation in the Greater Toronto Area and it's almost 65%, so on a really practical level, we think we should have some investigators and other staff on the ground in Toronto, and also to make connections with the stakeholder industry associations and, I guess, just to live and breathe the business, and understand the business in that area.

We also have an initiative going on in Saskatchewan where we have jurisdiction over businesses in that province. We're doing public education and compliance education in that province.

In British Columbia and Alberta, we have a lot of initiatives with our commissioner colleagues in those provinces because we share jurisdiction over the private sector. So we issue joint guidance to give more certainty to business and citizens in those provinces.

We also have a one-man band, as we call him, our outreach officer working in Atlantic Canada. He does a lot of public education and compliance education across the four Atlantic provinces.

● (1205)

Mr. Bill Siksay: Is that the only place where you have a specific staff person in a region?

Ms. Elizabeth Denham: That's correct. We predict that there will be five to seven people in the Toronto office who will do investigations and outreach.

Mr. Bill Siksay: Thank you, Chair.

The Chair: Ms. Davidson, please.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thank you very much, Mr. Chair.

Thank you very much for being here with us again today. It's always a pleasure to hear from you.

It's a particular pleasure today when I look at the wonderful report you've been able to give us on your accomplishments since the last main estimates. I think your department has definitely been working very diligently and has a lot of good accomplishments under its belt for this past year. I congratulate you and your other members on that.

My first question is on the Google issue. Of course, that is one of the things you've listed as one of your main accomplishments, and rightly so. I think you acted on that alongside other international heads of privacy agencies. How did you decide that it was your responsibility to be an international leader? Did you spearhead this? How did this come about?

Ms. Jennifer Stoddart: This particular initiative came about when I was with my international colleagues at an OECD meeting, which then coincided with discussions on the ongoing international conference arrangements. This international commissioners conference has been extant for some 25 years. Increasingly, all of the commissioners who are there are concerned about the same issues, because the same companies and the same types of technology affect all of our societies, which are western, European, Australian, New Zealand's, and so on. That's how it came about.

My office played a leading role for several reasons. First of all, we thought that a place to launch it would be at the conference for international privacy professionals, which takes place every year in Washington, D.C. We were obviously the closest people to Washington, and we were arguably more familiar with setting things up in Washington than the Italians, for example. We also function in two official languages, which is helpful for our colleagues in Spain, Italy, and France. There were considerations such as that.

Mrs. Patricia Davidson: That's good.

Did you say that you meet at this international commissioners conference once a year?

Ms. Jennifer Stoddart: Yes.

Mrs. Patricia Davidson: Is there a benefit, do you think, in meeting more often? Do you have other mechanisms to trade information and keep informed on what others are doing? I know that you talked a bit about the transborder complaint-sharing mechanism. I would expect that it's probably one way in which you and your international colleagues share information.

Do you think there's a need to do it more than is happening now? Is Canada more aware or less aware of privacy issues than the other OECD countries? Or are we all about the same?

Ms. Jennifer Stoddart: There are a lot of questions there.

Somebody who has been very active, because these issues involve private sector privacy, is assistant commissioner Elizabeth Denham. She's been involved in something called the Galway initiative. Could I ask her to assist us?

Mrs. Patricia Davidson: Sure.

Ms. Elizabeth Denham: I think our office has a lot of dance partners, internationally, when it comes to working on these issues that involve global companies. The Galway initiative is a joint initiative of U.S.-based multinationals, as well as European data protection commissioners and some academics. Again, we're looking at global privacy standards. How can we do this right and how can it make sense for companies so we don't have 27 different rules for transborder data flow? That's a bit of a think-tank initiative.

Another initiative, which is again through the OECD, is called the Global Privacy Enforcement Network. That group is now meeting a couple of times a year to get our heads around the consistent issues, the risks to privacy, and how we can have more of a global response.

There are quite a few initiatives going on. They're all aimed at looking at more of a standard approach to private sector privacy, something that's pragmatic and something that works for the way business operates and the new technology today.

● (1210)

Mrs. Patricia Davidson: Thank you.

Commissioner, we've heard from other commissioners that employees are hard to recruit, that they're perhaps hard to retain, and that it's difficult to maintain staffing levels. But in your comments, you say that “thanks to stable and appropriate funding”, you've been able to “attract and retain the full complement”. So you have that, and you have reached out to younger people; you made that comment as well.

Could you comment a bit more on the workforce and the balance you're trying to put in place?

Ms. Jennifer Stoddart: Some of the members of this committee will remember that we were in dire straits several years ago. We had the budget, but we would hire people and then they would leave. We didn't seem to be able to retain them and so on. Our director of human resources—who is here if you would like more details—put together a very comprehensive long-term recruitment plan.

We also looked at what a new generation of civil servants is looking for. Among other things, they're looking for interest in their job, trying to make a difference, and work-life balance. We try to stress these, not only in our recruitment, but in our personnel policies.

Over the last few years, as a whole generation moves to retirement, we have been able to recruit some very talented people. For the moment, they seem happy and not about to leave us.

Mrs. Patricia Davidson: That's good. Has this been a long-range plan?

Perhaps I could ask Tom—

Ms. Jennifer Stoddart: Yes.

Mr. Tom Pulcine (Director General and Chief Financial Officer, Corporate Services Branch, Office of the Privacy Commissioner of Canada): When the plan was first developed, I think it was over three or four years, so it is a long-range plan.

As the commissioner made reference to, it touches both on the recruitment issues and the retention issues. As it has evolved in our office over the last two years, I think there has certainly been more focus on the retention than the recruitment. Whereas in the previous two years there was probably a lot more focus on the recruitment side, now it's certainly more focused on the retention.

Mrs. Patricia Davidson: Do all the changes with the social media impact your long-term staffing plan?

Mr. Tom Pulcine: In terms of certain aspects, for sure. For example, we put a video on YouTube to try to attract people to our office. I guess the short answer to your question is “yes”.

Mrs. Patricia Davidson: Thank you.

The Chair: Thank you very much.

Ms. Simson, please.

Mrs. Michelle Simson (Scarborough Southwest, Lib.): Thank you, Chair.

Thank you, Ms. Stoddart. It has been a while, but I find your sessions informative, and I, too, want to add my voice to the congratulations for the work you did on Google.

I want to turn to something that's of particular interest to me. I've written your office and I know you've done a lot of good work on this. It's with respect to finding the delicate balance between national security issues and even, say, a tough-on-crime agenda...balancing obvious security issues with the right to privacy.

I just wanted to ask you if you familiar with the U.S. practice that was implemented post-9/11, fairly shortly after that, whereby the U. S. federal government, in the name of national security, had the ability to intercept communications that might or might not have links to terrorist activity and to retain information on individuals as a result of those intercepts.

The practice has been called the “special access program”. Are you familiar with it? If so, do you know if that has any implications for Canadians?

● (1215)

Ms. Jennifer Stoddart: Thank you.

If I may, Mr. Chair, I would ask Assistant Commissioner Bernier, who has a long experience in national security issues, to speak to that.

Ms. Chantal Bernier: In Canada, of course, as you know, the efforts in that regard took the form of Bill C-46 and Bill C-47, which died on the order paper. That would not allow interception of communications without a warrant. What that would allow is for an Internet service provider to give the law enforcement authorities or national security authorities the customer name and address behind an IP address. That is the effort that the Canadian government has made to have some widening of—

Mrs. Michelle Simson: Does your office have any specific concerns with respect to that piece of legislation?

Ms. Chantal Bernier: We have two main concerns. There are more details in the letter that I referred to earlier.

The two main concerns are this power to get from Internet service providers, without a warrant, a customer name and address, and second, we find that the oversight governance structure provided for in these pieces of legislation is not clear and perhaps not as independent as it could be.

Mrs. Michelle Simson: Is there something that your office could have done? I'm curious. We're seeing with this type of legislation and the tough-on-crime agenda the government has that certain aspects of bills may or may not tip the balance. What I'd like to find out is whether your office is ever consulted in the drafting process of some of this legislation. Are you asked for feedback as to potential problems this could pose down the road, unforeseen problems that are not apparent at the drafting stage?

Ms. Chantal Bernier: It depends. For example, through the privacy impact assessment review process, the RCMP will submit some initiatives to us. We review them to ensure that privacy is respected. We will make recommendations and we are often very successful.

Mrs. Michelle Simson: But in the legislative drafting process—

Ms. Chantal Bernier: In the legislative drafting, sometimes we are consulted, but in the case of Bill C-46 and Bill C-47, we had been consulted throughout the years in the preparation of this legislation. But then it was tabled and we reacted after it was tabled.

Mrs. Michelle Simson: Is there anything specific that you could do with that legislation that would perhaps add a little more balance or give a little more comfort to Canadians?

Ms. Chantal Bernier: We have made specific recommendations. We have specifically asked that the authorities who request these powers justify why they need them with greater clarity. We also requested that there be more definition around the oversight process.

Mrs. Michelle Simson: I did express this in a letter to the commissioner. For all intents and purposes, it looked like a great piece of legislation with respect to anti-money laundering legislation and terrorism. But it rolled into the fact that ordinary Canadians, in the course of buying a house, have to release their social insurance number, which can be stored God knows where and in God knows what way. Because of the identify theft issue, which has become a huge issue, that wasn't necessarily a good thing.

Would it be a good suggestion that we have a little more consultation with your office when we're drafting legislation of this kind to avoid these kinds of unanticipated results?

● (1220)

Ms. Chantal Bernier: Absolutely, and some departments do that. I think it's fair to say that in the end they benefit from it as much as Canadians, because we provide advice and they can therefore change their draft legislation and make it more privacy sensitive—

Mrs. Michelle Simson: Before it's tabled.

Thank you.

The Chair: Mr. Rickford, please.

Mr. Greg Rickford (Kenora, CPC): Thank you, Mr. Chair.

Thank you to the witnesses.

I, too, would like to congratulate you on your hard work, particularly in eliminating the backlog. Congratulations on that.

Just as a reminder, I noticed that you're doing consults in three cities, in Toronto, Montreal and Calgary. Of course, we'd always welcome you in the great Kenora riding, and it would be good, unlike previous governments, to pay some attention to some of the rural and remote areas that can no doubt make a good pitch on this issue.

I want to talk about estimates. Your report on priorities and planning—hereinafter RPP—indicates proposed increases in planned spending this year related to the implementation of the Electronic Commerce Protection Act. Your office was recently before us on the supplementary estimates (C) for 2009-10 with, I believe, a $100,000 item that was also linked to this implementation.

My questions are as follows. I'll just put them out there.

The Electronic Commerce Protection Act is Bill C-27 from the second session of the 40th Parliament. As of the date of publication of your RPP, it has not been reintroduced into the House during the third session, so how are you calculating implementation costs over a three-year period for a bill that has not yet been introduced?

Second, in your testimony to the committee on the supplementary estimates (C) for 2009-10, when you were here in March, you stated that the $100,000 allocated for this item has already been spent. Is this your projected future spending for the same kinds of activities on which that $100,000 was spent or for something else?

Finally, do you plan to include requests for these extra amounts in the upcoming supplementary estimates later in this fiscal year?

I'd be happy to repeat any of those questions if you didn't get them.

Ms. Jennifer Stoddart: Thank you.

I will start, and then I will ask our chief financial officer to continue, because these are fairly specialized issues of public accounting and I know that we have some accountants here.

Mr. Greg Rickford: Sure. I can appreciate that.

Ms. Jennifer Stoddart: First of all, my understanding is that at the time we published the report you referred to, it was planned that ECPA would pass the House at that time, so we were required to put it into our main estimates for the year. You'll see, though, that it's kind of highlighted in italics.

We then had to appear before you last month in what I think was a rather confusing exercise for everybody, perhaps, because they were still there in the main estimates, but the legislation had not been reintroduced. So that amount of money, as I understood then, vanished.

It is put there because of what I explained to you previously. It was at the Senate when Parliament was prorogued. We understand that it will be reintroduced. At that point, that money would be added to our main estimates. If it is not reintroduced this year, then we will never have that money. So we will continue, as long as we are told that there is planned legislation, to put in the planned amount that we would hope to spend if the legislation came into force.

Do I have it right there?

Mr. Tom Pulcine: Yes, for the most part. The one thing I would add is that in the reports on plans and priorities, which is the estimates that are before you, if you look at the financial resources, it identifies for the Electronic Commerce Protection Act amounts over the next three fiscal years, including this fiscal year. For 2010-11 we've identified a requirement for $849,000. For next year, for 2011-12, it is $2.1 million. That number remains at $2.1 million into the future, so it's for 2011-12 and ongoing.

In terms of the FTEs and our people involved this fiscal year, if the legislation were reintroduced and passed, we would be seeking resources, presumably under the supplementary estimate process, for those amounts of moneys that I just indicated. As well, in terms of FTEs, it's four this year and six for next year and the years after that.

Although $100,000 was allocated through the supplementary estimate process, because the legislation did not pass or receive royal assent, it has been placed in a frozen allotment, and for all intents and purposes it has lapsed and is gone forever. We will not see any financial benefit of that $100,000.

● (1225)

Mr. Greg Rickford: How much time do I have left?

The Chair: You have one minute.

Mr. Greg Rickford: Okay. I'm going to try to get to my next set of questions.

It looks as though you're devoting a considerable amount of your office's resources—just over $5 million, I think—to program activity 2, which entails actions such as preparing policy briefs, collaboration with other authorities, and conducting public consultations. Why are these activities listed separately from program activity 3 in the RPP public outreach? Would a public consultation not be a form of outreach to the public? I have a question following that, but I don't think I'll have time to get it in.

Ms. Jennifer Stoddart: We're trying to give Parliament as much detail as possible in distinguishing the work that is necessary to follow laws, technologies, human problems, or social trends in terms of privacy. We need to know what's happening, we need to analyze them, and we need to see how they fit in—or not—with Canadian law. So that's more the policy research development.

Secondly, we need to take the results of that and the best advice that we can give and reach out to Canadians by appropriate means. I think that's a quick way of describing it.

Mr. Greg Rickford: Thank you.

The Chair: Thank you.

Madame Freeman, s'il vous plaît.

[*Translation*]

Mrs. Carole Freeman: Before I pick up where I left off earlier, I want to ask Ms. Stoddart something.

In her April 21 report, the Auditor General of Canada, Sheila Fraser, talked about ageing information technology systems. Were you aware of the situation?

Ms. Jennifer Stoddart: No, we are responsible for our office and —

Mrs. Carole Freeman: But these computer systems store all the data. There are most certainly huge quantities of personal information at stake. I think there is reason to worry.

Do you intend to address the problem?

Ms. Jennifer Stoddart: Yes, some of our audits will probably focus on that. I will ask Assistant Commissioner Bernier to answer that question.

Mrs. Carole Freeman: It involves all the infrastructure that stores the personal information of every Canadian.

Ms. Chantal Bernier: Yes. It is the container for what we work to protect. We are addressing the matter in a number of ways. First, we are carrying out two audits on wireless communications and electronic infrastructure. And, as part of our review of privacy impact assessments, we are focusing on specific security concerns. Finally, we established a dialogue with Public Safety Canada's cybersecurity unit to strengthen our relationship and complement our work in that area.

Mrs. Carole Freeman: You are taking all of those steps, but the computer system is no longer adequate. What are you going to do if it fails?

Ms. Chantal Bernier: According to our mandate, we work on a case-by-case basis. For example, if one of our investigations reveals weaknesses in a department's electronic infrastructure, we make recommendations. Our annual report identified two cases where our recommendations led to better electronic infrastructure.

Mrs. Carole Freeman: What was done exactly?

Ms. Chantal Bernier: In one case, a department had a leak of personal information. We realized that access procedures were not adequate, so much so that over 1,000 people had access to the personal information of a single Canadian who was in custody abroad. Obviously, that is inappropriate. We made recommendations, and limits were placed on access. In another case, also mentioned in our report, a department was the victim of a cyber attack, which jeopardized the security of 60,000 people's personal information. In that case, too, the department took measures to strengthen its electronic infrastructure on its own.

● (1230)

Mrs. Carole Freeman: In Ms. Fraser's report, it says that the Canada Revenue Agency, Public Works and Government Services Canada, Human Resources and Skills Development Canada, the Royal Canadian Mounted Police and Citizenship and Immigration Canada were singled out in her review. I am not certain, but I would say those institutions have a lot of information. Have you done any specific monitoring of these institutions?

Ms. Chantal Bernier: First of all, every privacy impact assessment, in other words, the assessment that departments or agencies are subject to when implementing a program or policy, includes a security component. So we ask serious questions about that.

Second, we take note of any vulnerabilities for our audit plan, which is based on risk. And, clearly, we take those factors into account when choosing which audits to do next, precisely to ensure we are focusing on areas that present risks.

Mrs. Carole Freeman: Do you audit all agencies systematically?

Ms. Chantal Bernier: Not systematically, no, but we perform audits in cases where we think it is the most relevant. An audit—

Mrs. Carole Freeman: Pardon me, Ms. Bernier, but what relevance criteria do you use when deciding to focus on the RCMP rather than the Canada Revenue Agency, for example?

Ms. Chantal Bernier: When deciding where an audit is needed most, we look at the volume of information the institution has, as well as information disclosure practices and risks. Of course, we take into account the number of complaints in an area and the nature of the personal information being collected, among other things. As I said, volume is a factor. All of that goes into selecting the organizations we feel are most at risk.

Mrs. Carole Freeman: Have any of your recent assessments focused on the places I mentioned earlier?

Ms. Chantal Bernier: The most recent were, as you know, FINTRAC and Transport Canada, with respect to the passenger protect program, which includes the no-fly list. In the past, yes, the Canada Border Services Agency has been the subject of an audit and follow-up. In our annual reports, Passport Canada was identified, and the RCMP was the focus of a specific report on all exempt banks. Yes, we absolutely focused on those areas.

Mrs. Carole Freeman: Given what Ms. Fraser revealed in her report, do you intend to take any specific measures?

Ms. Chantal Bernier: Of course, that is a key consideration for us, and we will definitely take it into account when establishing our audit plan.

Mrs. Carole Freeman: Will it become your fifth priority?

Ms. Chantal Bernier: It is part of our information technologies priority.

Mrs. Carole Freeman: The chair is telling me that my time is up, Ms. Bernier. I apologize. Thank you for the information.

[*English*]

The Chair: We may give you a chance to come back to that again.

Mr. Siksay.

Mr. Bill Siksay: Thank you, Chair.

Commissioner, I've just looked at the package that you left today. Thank you for that information on camera surveillance, but thank you for the calendar, too. It's a lot of fun, so I very much appreciate it.

Voices: Oh, oh!

Mr. Bill Siksay: It's going on my desk.

I wanted to ask about the situation around whole-body scanning. I know you've done some work on it. Recently, I gather, there has been some...well, there's always a lot of activity around this. I think the transport committee is actually looking at it right now and has had some interesting testimony.

But two things have caught my eye recently. One is the experience of Schiphol airport in the Netherlands. They've put in place some further requirements around whole-body scanning that remove even the direct connection between the person reviewing the scan and the person being scanned. It makes it even more indirect, but still, apparently, effective. Also, in the United States, I gather that the Department of Homeland Security was recently petitioned by a number of privacy and civil liberties organizations, who were citing a whole range of privacy concerns, to stop the deployment of whole-body scanners.

I'm just wondering if any of those reports or that other work is causing you to take a further look at this. Or are you doing an ongoing watch on this subject?

Ms. Jennifer Stoddart: Yes. Thank you for the question. We do have an ongoing watch on this subject.

I'll just make two quick comments and then once again refer it to my very able assistant commissioner, who works on the national security issues.

We did look at the report analyzing the whole-body scanners in Schiphol. Interestingly enough, some of the information that came out of that test was that some people, particularly some women—stewardesses—preferred, in the context of security clearances to board planes, something like a whole-body scanner rather than being patted down, which for some people, particularly people of certain religions, can be felt as very intrusive. That gave us an interesting perspective on it.

Secondly, yes, we do watch what happens with our colleagues in Homeland Security. This is what happens in Canada now. There is no direct eyesight: there's Joe or Jane going through the scanner. I think there are some cartoons to that effect in our calendar, because we have to keep a sense of humour about all this. There's no direct line of vision in Canada. That's our understanding.

As for Homeland Security, my understanding is that they have a more powerful type of scanner than we have in Canada.

Is that true, Chantal?

● (1235)

Ms. Chantal Bernier: There are a few things.

First of all, we are considering this a watching brief, and we have received assurances from CATSA that they will look at every possible technology that could make this less privacy-intrusive, such as the possibility, one day, that it not be seen by a human being. They have already told us that they're looking into that.

In relation to the U.S., as the commissioner has mentioned, they do not have quite the same policies that we have. In fact, the privacy advocates in the U.S. have called for exactly what has been implemented in Canada, meaning optional.

Mr. Bill Siksay: Okay. Thank you.

In the documentation you provided, the analysis of your employment equity group shows that you're doing very, very well in that regard. Certainly in all categories you're either above or at the level of Canadian labour market availability. I think that's something that again you need to be congratulated for. I'm sure it's a stellar record in terms of other departments and agencies.

But I wanted to ask if you do any specific gender analysis in terms of the issues that you're working on. There has been some reporting with regard to social media that women and young women participate more in that. I'm wondering if you do that kind of gender analysis of the issues that you're working on and if it's leading you in any particular direction on any specific issues.

Ms. Jennifer Stoddart: Yes, I'd say that often we do. We do try to isolate the gender factor, particularly in terms of how to target our public information and what might be the particular slant in some of the youth focus groups that we had. We're not, for the moment, but I'm kind of looking for additions here.

We haven't had a kind of gender and privacy program, but I certainly remember that when CATSA said that it was going to move toward these scanners and we received a PIA, I said that I wanted women on the team. I said that I wanted women to go out and report on that, because this kind of thing can be potentially more sensitive to women and to other groups than it may be for your standard man.

I don't know. Are there other gender-based...? The fact that we are—unusually—three women means that we do try to keep this in mind.

Mr. Bill Siksay: I also wanted to ask about this. I know that you're doing consultations and that one of the consultations is around profiling of consumers by business and online monitoring and those kinds of consumer issues. One of them that I have been aware of recently is the use of online coupons and the information about consumers that this transfers to businesses, often without the consumer knowing that.

I'm just wondering if that's something specific that you're looking at or if that will come up as part of these consultations. Or is that the kind of thing that you're even hoping is raised at these consultations?

Ms. Jennifer Stoddart: Yes. Thanks. I just heard about this myself, but Assistant Commissioner Denham has been organizing these consultations.

Ms. Elizabeth Denham: I think the issue of online coupons is going to be addressed, because what we're trying to do is understand how this information is collected and how transparent that collection is. Do consumers really understand how much of their data is collected by advertisers and third party advertisers through various means, including coupons? So yes, we're very anxious to participate and hear about all the methods of collecting personal information online.

● (1240)

Mr. Bill Siksay: I have one other very quick question. It has come across my desk recently that some American states have passed laws around the implantation of microchips in human beings. I'm wondering if that's something that has crossed your desk or if it's something on your radar. Is it something that you've heard about?

Ms. Jennifer Stoddart: Oh, yes, it's definitely on our radar. One of the things that helps to keep us informed is that we get virtual press clippings now. We subscribe to periodicals and news feeds. This came up five or six years ago, I think. Even before that, in 2001, I remember that Agriculture Canada and the provinces were moving to chips in animals, so it wasn't far from there to chips in people.

It's on our radar screen. We don't have any complaints, as far as I know. We're not specifically discussing chipping. There is some discussion that for certain people, such as those with Alzheimer's disease, for example, this might be a device that would be fairly benign. But we'll continue to watch it.

Mr. Bill Siksay: Thank you.

The Chair: I have Ms. Davidson, Mr. Easter, and Madame Freeman for a small follow-up. Unless anyone else wants to be added to the list, that will be it.

Ms. Davidson, please.

Mrs. Patricia Davidson: Thank you very much, Mr. Chair.

Commissioner, when I was looking on your website, I saw a statement that I'm going to read for you, because I won't remember it exactly if I don't read it. It says:

> Globalization raises the challenge of trying to find a cross-border privacy language. Technological advances hold out the promise of greater convenience, but sometimes at a cost to human rights such as privacy and the ability to control our personal information.

That's the quote from the website. Do you really think that a cross-border privacy language is possible for everyone on the Internet?

Ms. Jennifer Stoddart: I guess I'm talking particularly about regulatory authorities, various organizations that different governments have tasked with trying to regulate cross-border privacy. Yes, I do think it's possible.

In the time I've been in this field, I think we've made quite a bit of progress on moving together approaches to the regulation of personal information, particularly online. There's an intense dialogue going on now between the European Union, as it's being restructured after the changes in the Lisbon treaty, and the United States, about parameters for exchange of cross-border personal information, both in the national security setting and in the consumer setting.

So yes, the good news is that while the technologies continue, the dialogue has never been, I think, as productive and congenial.

Mrs. Patricia Davidson: Thank you.

When you're dealing with large companies, do you have any worries about the regulations or the rules that you have to impart to them about how they're going to operate? Are they more concerned, in most cases, about business rather than privacy? Or are you finding that it's a good mix and there's good compliance?

Ms. Jennifer Stoddart: Yes. I believe that large companies in Canada have done quite a good job of implementing privacy.

Remember, one of the big sectors that we regulate is the financial and banking sector, and I think in Canada we saw during the recent economic upheavals that we have some very positive traditions in our banking and financial community. Confidentiality is one of them.

Generally I'm very happy with the uptake by big business. What is of greater concern are medium-sized and small businesses and the possible costs to them.

I'm not necessarily saying that privacy is a huge cost, but I think that sometimes there are some very enterprising people who can sell to small or medium-sized businesses a package that is unnecessarily expensive. I've heard some of them complain about that, so we've tried to focus in a section of our website on small business and what we can do for them. We're bringing out a whole new package—I think within the next month and a half—to update how small and medium-sized businesses can do privacy for themselves, at a minimal cost, without going through expensive services.

● (1245)

Mrs. Patricia Davidson: Thank you.

The Chair: Thank you.

We'll go to Mr. Easter, please.

Hon. Wayne Easter: Thank you, Mr. Chair.

I know, Commissioner, that you've done a lot of work on Google and Facebook—good work. But I have a concern. I use Facebook. A lot of us do around here. There certainly is, as you've indicated, legitimate concern about the material on there, which might not cause individuals a problem today but might 10 years down the road. How do you get the message out there on the potential dangers of using Facebook in a certain way?

I'm a member of Parliament, and to be quite brutally honest with you, until I was appointed to this committee, I was not aware of the work that you've done in this area. We are all involved in our own committees and are running hell west and crooked, and sometimes things pass us by.

I think increasingly with younger folks, who are huge users of the system, how do you get the message out? What can governments do to basically assist you to get information out there on what people have to be careful of?

Ms. Jennifer Stoddart: Thank you for that question. I think it would be wonderful if all the government departments and agencies could reinforce our message. I know that on most government websites now you can see the privacy policy; it's a Treasury Board requirement and so on.

Assistant Commissioner Denham, who's in charge of the Facebook file, may have other things to say, but we try to do two things.

First of all, specifically to reach out to young people, young and younger adults, who are intensive users of these new social media, we've started a youth privacy website that is reachable from our main site. We have a youth blog.

We've worked with an educational association to develop materials for teachers. The teachers can then apply to that association and use that. We have an annual video competition for young people. They make videos on privacy. We just announced last year's winners.

We have a huge emphasis on youth in our materials.

More generally, I think we're being forced to go to the non-traditional world, the traditional world being the annual report to Parliament, the learned reports, and so on. Those are still extremely important, but to get to the population, particularly to a certain demographic, we go through online media. That's not even radio—I understand that some people don't listen to radio anymore. It's television. They will listen to television, because then the clips can be downloaded and played. We use YouTube. Tom Pulcine mentioned what we're doing on YouTube. We're on Twitter. We're working through the media where young people are.

The Chair: Thank you.

Madame Freeman, s'il vous plaît.

[*Translation*]

Mrs. Carole Freeman: I want to take my colleague's question a step further.

In U.S. airports, they are already using fingerprints to scan people. They are also talking about using iris recognition as a means of identification. What is your position on that?

Ms. Jennifer Stoddart: In Canada, I think we are already using iris recognition as a means of identification under the NEXUS program, for example. We believe the utmost care and caution needs to be exercised when using these technologies. I believe we have done a few audits on such programs. We are not adamantly opposed to them, in that a large number of Canadian passports are falsified and there is a large market for stolen Canadian passports. When used properly, this technology enhances identity protection. However, those using the technology have to be extremely conscientious. Safety measures are necessary, especially to prevent digital images from being stolen.

● (1250)

Mrs. Carole Freeman: Do you mean iris recognition or fingerprints?

Ms. Jennifer Stoddart: I was talking generally about both.

Mrs. Carole Freeman: In all honestly, I find that troubling and unacceptable. In my view, it is an intolerable intrusion. There are advertisements for Montreal airport boasting that this method of identification is modern, but I feel that I am in a...I cannot conceive how we got to the point of making methods like that so commonplace.

Ms. Jennifer Stoddart: We are—

Mrs. Carole Freeman: You are still using it and saying that it is to increase security. That is always how our privacy is trampled on: by pretending that it increases security. In a way, I can take care of my own security. It astonishes me that you find iris recognition normal.

Ms. Jennifer Stoddart: I am not saying that it is normal. I do not believe that I used that word.

There are two types of security: physical, national and military security and the security of one's identity. Identity theft has been on the increase for 10 years and it is common now. We get to that stage not only because of security issues. Waves upon waves of people are walking around the world using false identities. In that sense, it is a major problem. It is a problem in cybercrime, for example. People wanting to come to Canada pretend to be other people. These new technologies—

Mrs. Carole Freeman: I think I understand where your thinking is headed. Would you go as far as to say that taking people's fingerprints would become something as normal in Canada as it is in the United States?

Ms. Jennifer Stoddart: I never said that it is something normal.

Mrs. Carole Freeman: Let us say “usual“.

Ms. Jennifer Stoddart: I think that Canadian passports are eventually going to go in that direction. Is there going to be optical scanning?

Ms. Chantal Bernier: We have looked at the privacy assessment of the smart Canadian passport as currently proposed. It will contain a chip that has no more information than page 2 of the passport currently does.

Mrs. Carole Freeman: That has nothing to do with the iris.

Ms. Chantal Bernier: No. There is no iris scan in the smart passport.

Mrs. Carole Freeman: So at what point will iris recognition be used?

Ms. Chantal Bernier: In the assessments that we are doing at the moment, that is not what departments are proposing. They have not proposed using iris recognition as a means of identification.

Mrs. Carole Freeman: But Montreal airport is advertising it.

Ms. Jennifer Stoddart: That is a special program called NEXUS, and it is completely voluntary.

Mrs. Carole Freeman: It is voluntary?

Ms. Jennifer Stoddart: I was at Montreal airport recently on my way back from Washington. I heard two businessmen talking. One was saying that he thought that signing up for the Nexus program was great because everything moves much more quickly.

Mrs. Carole Freeman: Thank you.

Mr. Chair is indicating that my time is up.

[*English*]

The Chair: Yes. Mr. Siksay can honestly say that he doesn't abuse his schedule. I'm not sure that you can use that excuse—

Voices: Oh, oh!

The Chair: —but it evens out over time.

We have only a few minutes and we do have motions to deal with and a couple of other things.

First of all, I want to thank you, Commissioner, and your whole team for keeping us apprised of a very broad scope of issues. I was thinking about it during the meeting and getting a little concerned about our ability to keep up, to support you, and to be engaged. I think that over time, particularly with the emergence of Facebook—this is probably the tip of the iceberg—committees such as ours may not be able to handle four commissioners; we may need to have two commissioners—and we'll still be very busy. We'll have to watch for this.

I should mention to everyone that April 30 is the deadline for the Minister of Justice to respond to our committee on quick fixes on privacy, as well as to our report on access. I have not received those responses yet. I will prompt again.

As soon as we get them, Commissioner, we will certainly make sure that you also have a copy of the minister's responses.

Colleagues, we have to pose the motion on the estimates, so I'll put it now.

Shall vote 45 under Justice, less the amounts voted in interim supply, carry?

JUSTICE

Offices of the Information and Privacy Commissioners of Canada

Vote 45—Office of the Privacy Commissioner of Canada—Program expenditures.....$20,099,000

(Vote 45 agreed to)

The Chair: Shall I report the main estimates to the House?

Some hon. members: Agreed.

The Chair: Thank you kindly.

Thank you to our witnesses and to all of our colleagues.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

PERMISSION DU PRÉSIDENT

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca