HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 054 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, November 1, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 1, 2012

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Order, please. We will now get started.

As you can see on our agenda, we will continue our study on privacy and the social media. We have witnesses from two organizations: Mrs. Tallim and Mr. Johnson from MediaSmarts—or *Habilomédias* in French—as well as Professor Bennett from the University of Victoria, who joins us by videoconference from Victoria, B.C.

As usual, each witness will have 10 minutes for a presentation. This will be followed by a period of questions and answers.

I will now give the floor to Mrs. Tallim and Mr. Johnson from MediaSmarts.

[*English*]

Ms. Jane Tallim (Co-Executive Director, MediaSmarts): Thank you very much.

Hello, I am Jane Tallim, co-executive director of MediaSmarts. With me is Matthew Johnson, who is our director of education and resident privacy expert. Thank you so much for inviting us here today.

We've been following the testimony to this committee with great interest and the many excellent recommendations that you've received so far. We've also noticed the number of expert witnesses who have stated that education, especially for children and youth, is an essential part of a comprehensive approach to addressing online privacy issues.

With this in mind, we would like to focus our remarks on how digital literacy, and in particular privacy education, can help young people develop good privacy habits for social media and other online activities.

Today's presentation is very timely because next week is Canada's annual Media Literacy Week. It's co-led by the Canadian Teachers' Federation and us. This year's theme is “Privacy Matters”. On Monday we'll be in Montreal hosting a youth panel exploring this topic to launch the week.

For those of you who aren't familiar with our organization, MediaSmarts is a national not-for-profit centre for digital and media literacy. We work to ensure that children and youth have the critical thinking skills to engage with media as active and informed digital citizens.

We were launched in 1995 as Media Awareness Network through a CRTC initiative on television violence. The commission's policy on this issue stated that although industry self-regulation and TV classification systems would play a role, public awareness and media literacy programs represented the primary solution to TV violence.

The same thinking applies today to online privacy. Given the inherent difficulties legislators face keeping up with constantly evolving platforms and applications, education plays a critical role in helping Canadians of all ages understand their rights and manage their privacy and personal data.

Digital literacy is the term we use to describe the range of skills needed by young people to make wise, informed, and ethical online decisions. Privacy management is one of these core skills.

Our digital literacy resources and programs are informed by our ongoing research project, Young Canadians in a Wired World. This is Canada's longest running and most comprehensive investigation of the behaviours, attitudes, and opinions of Canadian children and youth with respect to their use of the Internet.

One of our key areas of inquiry is young people's understanding and behaviours relating to online privacy, including the types of privacy invasions they encounter, and the role of adults in building awareness and influencing behaviours.

We recently launched phase three of the young Canadians project with funding from the Office of the Privacy Commissioner of Canada. Dr. Valerie Steeves of the University of Ottawa, who is our lead investigator, presented our qualitative findings to this committee in May, so you've already had a snapshot of how online surveillance has become a reality for today's youth.

Although young people find the constant surveillance annoying, persistent myths about stranger danger and Internet risks encourage them to buy into the idea that they need to be monitored to keep them safe online. The constant surveillance by parents, schools, and corporations, and young people's acceptance of it is cause for concern. Privacy is a fundamental human right, and continuous surveillance chips away at our private space. Moreover, this constant scrutiny undermines the mutual trust, confidence, and communication between adults and youth that is essential to giving young people the autonomy they need to develop digital life skills.

Finally, if youth grow up in an environment where surveillance at home and at school is normal and accepted, they are less likely to be aware of or to exercise their privacy rights regarding corporate surveillance.

We're going to be heading into classrooms across the country next February with our national survey to explore many of the privacy issues that emerged in the qualitative study. Specifically, we want to learn where the gaps are in digital literacy skills so we can address them in educational materials for classrooms and communities. For example, we'll be asking students if anyone has ever taught them how to read privacy policies or terms of use on websites.

Drawing from past young Canadians research findings, we have developed an extensive collection of resources on privacy management, ranging from games to teach good privacy habits to young children, to a comprehensive professional development workshop that trains teachers in how to address and improve the state of privacy as it pertains to the online activities of their students.

● (1535)

In our educational materials we focus on encouraging youth to make good choices about their own privacy, and also on teaching privacy ethics. Not only is it important to have our privacy respected and protected, we need to respect and protect the online privacy of others. This idea is most immediately relevant when it comes to social interactions online, but it has implications for corporate uses of privacy as well. One reason we place privacy education in the context of digital literacy is that, as other presenters have noted, privacy is not a stand-alone issue. It intersects with safety, cyber security. cyber bullying, authentication of information and digital citizenship.

An important part of digital citizenship is understanding and exercising your rights, both as a citizen and a consumer. To do that, youth need to know that their personal information has value and that they have legal and contractual recourse in protecting it.

Perceived importance of information privacy is a critical factor in determining how well young people manage their online privacy. With children going online at increasingly younger ages, this sense of that personal information is valuable and belongs to oneself is important to cultivate, even at the primary level. For example, we have a Privacy Pirates game on our website, which was funded by Google. It helps younger students start to understand this concept.

Support for the critical importance of privacy education for youth has precedent in Canada and internationally. In 2008, Canada's privacy commissioners and privacy oversight officials passed a resolution on children's online privacy, where they committed to improve the state of privacy as it pertains to the online activities of children and youth by implementing public education activities to increase their awareness of online privacy risks. Since that time, the Office of the Privacy Commissioner has produced several excellent educational resources and has funded organizations, including ours, to produce privacy education materials.

In February of this year, the OECD adopted a recommendation on enhanced children's online protection, recognizing that the protection of children online encompasses content risks, contact risks, consumer risks, and risks relating to information security and online privacy. The OECD recommends that national governments foster awareness raising and education as essential tools for empowering parents and children, and develop responses that include all stakeholders, and integrate a mix of public and private, voluntary and legal, awareness raising, educational, and technical measures.

Good comparative models for Canada are Britain and Australia. Both have strong digital literacy components in their national digital strategies. In Australia, the federal regulator, ACMA, produces many resources addressing children's online privacy concerns. In the U.K., they've coined the notion that Britons should bear a digital entitlement, which includes not only access but also the right to basic digital literacy skills, including privacy.

The notion of privacy education for all is essential to fostering informed citizens who recognize and challenge invasive practices online. As several witnesses have noted, when the public pushes, the industry tends to pull back.

It's a widely held belief that young people, whether they be Facebook addicts or aspiring YouTube celebrities, don't care about privacy. This isn't true. In fact, the way youth understand privacy may be more relevant than how most adults view it, because they see it not as a matter of deciding whether or not to share, but as having control over the things they want to share.

To support youth, we need to widen the current focus on privacy safety risks to include privacy rights, ethical use, recourse mechanisms, and the civic and democratic dimensions of privacy. Privacy education must be supported on a national level, both through the K to 12 curriculum in schools and public awareness campaigns to inform ail Canadians.

Thank you.

● (1540)

[*Translation*]

The Chair: Thank you very much for your presentation.

We will now hear Mr. Bennett, live from the beautiful city of Victoria, B.C., who will make a presentation. He is a professor at the University of Victoria.

Mr. Bennett, please. You have 10 minutes.

[*English*]

Dr. Colin Bennett (Professor, University of Victoria): Thank you very much. I trust you can hear me okay.

[*Translation*]

The Chair: Yes, I can hear you perfectly.

[*English*]

Dr. Colin Bennett: I thank you for the opportunity to appear before your committee and to speak about this important issue.

I am a professor of political science at the University of Victoria and have been studying privacy protection issues for nearly 30 years in Canada and internationally. I've written or edited six books on the subject and numerous articles. I'm currently in receipt of a grant from the Social Sciences and Humanities Research Council to study privacy protection of social media. I'm also working on this same subject under a contributions grant from the Office of the Privacy Commissioner of Canada.

The privacy questions raised by social networking services are broad and dynamic, as you've no doubt discovered. Social networking challenges some of the traditional approaches and assumptions behind our privacy protection laws. As you've just heard, it requires extensive education.

The Privacy Commissioner of Canada has already outlined the privacy principles that should apply to social media. Her office has been at the forefront of global efforts to ensure that big data companies abide by established privacy rules and practices. But social media is not just out there, and it's not just about Facebook, it's also about our own organizations and our own practices.

Rather than discuss social networking in all its manifestations, I want to address an area of social networking and privacy that is far closer to your own experiences and lives as politicians. I want to raise a set of questions about how your own political parties use social networking services, and indeed, other sources of personal information to build databases about Canadian citizens.

I have just co-authored a report on privacy in Canada's political parties for the Office of the Privacy Commissioner. This work was started back in 2011 and was published earlier this year. I'd like to take this opportunity to summarize the main findings, because I think this relates closely to the subjects of your inquiries.

Canada's federal political parties can and do collect a large amount and variety of information on Canadian citizens: on voters, volunteers, donors, members, and supporters. A disparate and fluctuating number of employees and volunteers might also have access to these data, individuals who may have no privacy and security training. Increasingly, these data are communicated through highly mobile and dispersed electronic formats, and increasingly, they are captured through the observation of social networking activity.

Canadian parties now operate extensive voter management databases; they have been doing so for some time. There are the Conservatives' constituent information management system, CIMS, Liberalist, and NDP Vote. The foundation of these databases is the electoral list provided under the authority of the Elections Act by Elections Canada, but upon that framework, a large and increasing range of other data about voters is added and analyzed.

These data come from a variety of sources: telephone polling, traditional canvassing methods, petitions, letters, commercially available geo-demographic and marketing databases, and indeed, from social networking services. Overall, however, for a variety of reasons, the contents of those systems are shrouded in some secrecy.

As new technologies pioneered in U.S. elections increasingly play a role in modern campaigning, so the range and variety of personal data available to parties will increase, and so will the concerns about the protection of personal privacy.

Here are some examples: smart phone applications for political canvassers; targeted online advertisement software; targeted e-mail campaigns, which match IP addresses with other data sets showing party affiliation, donation history, and socio-economic characteristics; sophisticated market segmentation strategies aligning online and offline behaviour; extensive use of robocalling and robotexting; and, of course, the use of social networking and social media to plan campaigns, to target likely voters and donors, and to measure impact and engagement.

Social media not only provide a convenient method to target likely supporters, but also to capture increasingly refined information about the preferences and behaviours of voters, and their contacts and their friends. These developments have received much attention in the current U.S. election cycle. One of the most notable trends is the increasing use of customized and targeted political advertisements based on the digital trails individuals leave through their social networking activities. A recent report suggests there were no fewer than 76 different tracking programs that were observable on www.barackobama.com.

Surveillance during Canadian elections is less extensive and is less intrusive—well, so far. Nevertheless there have been a number of recent controversies that have raised concerns about the practices of political parties and have raised the profile of this issue.

The Privacy Commissioner has also received a number of complaints and inquiries about the activities of our political parties over the last several years, and they've also been raised to some extent in the provinces. However, she can do little to address these inquiries because, unlike in most other democratic countries, Canadian federal privacy protection law does not cover our political organizations.

● (1545)

Parties do not engage in much commercial activity and are therefore largely unregulated under the Personal Information Protection and Electronic Documents Act, PIPEDA, or substantially similar provincial laws. They're not government agencies and therefore are unregulated by the Privacy Act. The only federal law that really governs their privacy practices is the Canada Elections Act, but that legislation only applies to those voter registration data collected and shared with parties and candidates under the authority of that legislation.

Parties are also exempt from the new anti-spam legislation, Bill C-28, as well as from the do not call regulations administered through the CRTC. Thus, for the most part, individuals have no legal rights to learn what information is contained in party databases, to access and correct those data, to remove themselves from the systems, or to restrict the collection, use, and disclosure of their personal data. For the most part, parties have no legal obligations to keep that information secure, to only retain it for as long as necessary, and to control who might have access to it.

Virtually every other public or private organization in Canada must abide by these basic rules, so why should political parties be different? Of course, I concede that political parties play a critical role in our democracy. Parties need personal information to mobilize and to educate voters and for a variety of other reasons, and it has been claimed that these important functions outweigh the arguments for regulation and that therefore voluntary self-regulation will suffice, but as our report demonstrates, the current voluntary policies of our main federal political parties are incomplete, and they are inadequate.

From the point of view of an ordinary supporter or contributor, or potential voter who wishes to exercise control over his or her personal information, the existing voluntary privacy commitments of Canada's main federal parties are often difficult to find, often inconsistent, and often somewhat vague.

No party is any better or worse than any other here—I'm not picking winners or losers—but there's little evidence, frankly, that any of your parties has given sustained consideration to privacy and to the risks associated with amassing vast amounts of personal data. For example, there's no link to privacy on the home pages of either the Liberals or the NDP, the last time I checked. There is a link on that of the Conservative Party, which is fairly prominent, but their policy is also somewhat incomplete, and it contains vague assertions and exemptions.

It would be my preference for Canadian federal political parties to be brought within the statutory requirements of PIPEDA and therefore under the authority of the Privacy Commissioner of Canada. I would urge the committee to consider that. However, in the meantime I think more can be done on a voluntary basis.

I think it would be a good idea—and I have read that some political parties have already done this, but it's not necessarily prominent—that all federal political parties declare that they voluntarily abide by the obligations in PIPEDA. It would be a good idea for them to revise their privacy policies and base them on the 10 privacy principles upon which PIPEDA is based, and to publish these more prominently. I think all parties should appoint a responsible official, the equivalent of a chief privacy officer, who would have overall responsibility for the collection, use, and dissemination of personally identifiable information. All political parties should adopt appropriate risk management strategies in case of data breaches. Data breaches are seen in many other areas of our life, in the public and the private sector. I think there should be training of staff and volunteers on privacy and security issues.

It may be that some of those activities are already occurring. I don't wish to be too critical, but my point is that it's not necessarily obvious, and therefore it's very difficult for individuals and ordinary voters and supporters, etc., to find out what their rights are.

These questions are not just about privacy. Lack of attention to the protection of personal information can erode the trust that Canadians have in the political parties and in our democratic system. In an age of social networking, being more proactive about privacy protection and providing those necessary assurances is also good organizational practice.

In summary, I applaud the committee's attention to these challenging issues concerning social media and to the practices of big data companies such as Facebook and Google. There's been a great deal written about that subject, and I can certainly talk about those wider issues. At the same time, little attention has been given to the questions that I raise here, which I think are very much related to the topic of your inquiry and, of course, to your own individual work.

I would encourage you, therefore, to think about what I've said and to work within your own organizations to get your own houses in order and to encourage your respective parties to follow the same set of information privacy principles that apply to most other Canadian organizations.

● (1550)

I fear that controversies about parties and privacy protection of voters will only continue. The appropriate management of personal data in an era of extensive online social networking is not only in the interests of individual citizens, but also in the interests of your own parties and of the long-term health of our political system.

Thank you very much for your attention.

[*Translation*]

The Chair: Thank you very much for your presentation. We can really feel the election fever in Victoria.

I will now give the floor to Mrs. Borg for seven minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair.

I want to thank the witnesses for being here with us today.

My first questions will be to the representatives of MediaSmarts.

We often hear in this committee that control measures should be in the hands of users. This is why we need an organization like yours. Indeed, you cannot give control to someone who cannot understand what is at play. People cannot use existing controls if they do not have a good understanding of how the web works. So we need to increase digital literacy.

Do you think Canada is doing enough to promote digital literacy to the young or to all citizens in general?

[*English*]

Ms. Jane Tallim: We are quite optimistic. We made a submission to the government consultations for the digital economy and are still quite hopeful that, as it has been in other countries, digital literacy will be a core pillar of any national strategy.

We were also very heartened in reading Janet Goulding's testimony, that she indicated the importance of digital literacy skills development throughout her testimony.

One of the challenges in Canada, though, is that education tends to fall provincially, and the federal agenda is a little different. We have all sorts of good work being done. For example, HRSDC focuses on work skills development. Really, we need some leadership in that public piece, that entitlement piece in the U.K. which I alluded to, as well as in ensuring that Canadian youth are also well equipped to be citizens in the digital world.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Do you have something to add?

[*English*]

Mr. Matthew Johnson (Director of Education, MediaSmarts): I'd like to add that you're absolutely right that simply providing tools to protect privacy is not enough.

We know this from a study that was done at Columbia University in the United States. It found that of the participants in the study, and these were students ages 18 to 25, 95%, or almost all of them, had changed their privacy settings on Facebook and felt confident that these settings reflected their desired privacy. However, when their profiles were studied, it was found that every single one of them had either shared things they did not intend to share, or in a lesser number of cases, had kept things private that they had desired to share.

Even though there is an awareness, and even if they have the tools, we know that the understanding of how to use those tools effectively does not come without education.

● (1555)

[*Translation*]

Ms. Charmaine Borg: In this regard, you mentioned that we need to educate the young and all users in general. Indeed, this is not simply a matter of age.

Who should be in charge of this? The private sector, social media companies or governments? How do you perceive the roles of the different stakeholders in this area?

[*English*]

Ms. Jane Tallim: Traditionally, the most effective responses are comprehensive partnerships. In its recommendations as well, the OECD was stressing the importance of having community, education, government, and the private sector work together to create these comprehensive approaches.

[*Translation*]

Ms. Charmaine Borg: Thank you.

You briefly mentioned the British model. Can you tell us why this model was so successful?

[*English*]

Ms. Jane Tallim: It is currently being evaluated, but in the U.K. they created the concept, as I said, of a digital entitlement. With that they've prevented the siloing of digital literacy skills development among the general public and their being classified as just work skills development.

There are many programs that were initiated in the U.K. There is Go ON UK, which is a foundation now, which has all sorts of training and educational resources for the general public. They are also very interested in reaching more vulnerable sectors of the public. They've created something that is a national campaign, which anyone can access and use.

[*Translation*]

Ms. Charmaine Borg: This is very interesting.

Some witnesses, including Valerie Steeves, talked to us about standards. In the development of standards, you would not necessarily want to simply prevent young people from using the Internet or social media because they have some benefits. As a matter of fact, they can be a source of learning, especially for the young. There are numerous examples of this.

In your opinion, what kind of standards should we have? Should the standards be different for younger people?

[*English*]

Mr. Matthew Johnson: Legislation may well play a role. Certainly our position is that young people do need to understand what they're agreeing to. They need to understand when they use any service what information they are giving out, what information about their activities may be collected, and what will be done with that information by either the operator of the service or third parties to whom it may be sold. How this transparency comes about may well be from a combination of legislation, industry regulation, consumer action, which we have seen has been very effective. However, in whichever case it is, we do need the additional pillar of privacy education so that young people are able to understand that this information is available to them and to make use of it in an effective way.

[*Translation*]

Ms. Charmaine Borg: So there is more than legislation. We should have a multifaceted program.

Do I have any time left?

The Chair: You have five seconds.

Ms. Charmaine Borg: Then, I am done.

Thank you very much.

The Chair: Mrs. Davidson, please, for seven minutes.

[*English*]

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

Thank you, presenters. Certainly it's an interesting topic that we've been studying for quite some time, and it's always interesting to hear different perspectives.

I'm particularly interested in the education of children and youth. An area that I don't understand very well is how the message is getting through to our children. When I look at my grandchildren, who are five and seven years old, how are they being taught? You talked about going into the classrooms next February. What grades do you target and what ages of children? What do you try to teach them? How do you impress upon a five-year-old what privacy even means?

● (1600)

Ms. Jane Tallim: With our young Canadians survey next year, we will be going into classrooms from grade 4 to grade 11. We will have a wide range of information. We do two versions of the survey: one for younger students in grades 4 to 6, and one for students in grades 4 to 11. Outcomes for various digital literacy skills, privacy included, are throughout the curriculum in Canada, but as you can imagine, it varies from province to province. That's one of the things we would really like to see leadership in. Some provinces do it better than others. Some provinces start with younger ages than others.

When she talked to you last spring, I think Professor Steeves mentioned that part of our qualitative phase of the young Canadians project was teacher interviews, which we did as well. The teachers had tremendous insight as well. Many of them really do want to start integrating technology into their classrooms in authentic ways so they can begin to develop these skills. Of course they also need training, support, and curriculum outcomes that give them some guidance as to what skills youth need.

I think there are pieces there. What's really needed perhaps is a comprehensive framework that looks at those core competencies that are needed relating to privacy education and other digital literacy skills so our teachers have some guidance and consistency in how they're taught.

Mr. Matthew Johnson: To add to that, you had asked how it is we can teach privacy skills to different ages. I'll answer, just from our perspective, that all of our resources are created by educators as well as by people who are experts in digital literacy issues, including privacy.

That means everything we do is based in part on our understanding of pedagogy and cognitive development. We base it on what young people are able to understand at different ages. Also, it comes from our own research and awareness of research being done around the world, so that we're able to listen to young people and know what it is they're concerned about in terms of privacy and other issues at different ages. We use that as a beginning point to get them interested.

That's a big part of our research. Why we conduct our research is to understand that, as has been shown again and again in research around the world, young people do care about privacy. To be able to make them aware of the issues, we have to talk about it in a language that is relevant to them.

Mrs. Patricia Davidson: That's a statement that we've heard over and over again, that young people do care about privacy. I'm really glad to hear that statement from different areas. It's not just coming from one source. That's very encouraging.

One thing I'd like to ask you about, though, further on the privacy issue with youth, is the consent forms and the privacy rules. I don't know too many adults, let alone youth, who can comprehend what any of these multi-page forms mean. Is there an effort to try to standardize something that would be more in a youth format?

Ms. Jane Tallim: That's something that is germane, and I know you've heard a lot of testimony about how you almost have to be a legal professional to understand many of the privacy policies. There is best practice out there. Sara Grimes alluded to a few children's sites that do an exceptional job. I think that's part of it. I think it's about lauding the companies that are very respectful, that try to be transparent, that put things up very clearly and are easily understood, that only ask for the most necessary information.

It's a combination of educating parents and educating children as well, so that young people who are too young to really understand what the big picture is can have a trusted adult with them, to help them go through it and understand. We have no problems with children having fun online, and most do in commercial environments. They're being sold to one way or another. The important thing is for children to understand that these fun playgrounds are there because companies want to sell them things. They can still have fun, but it's about developing that understanding.

● (1605)

Mrs. Patricia Davidson: You talked about the challenges of trying to get the same message out across the country. You talked about different standards in different provinces and different levels and ages of engagement.

What do you see as the federal role in this?

Ms. Jane Tallim: The federal role can provide leadership in supporting gatherings, events, facilitating opportunities for multiple stakeholders to come together and conceptualize what this framework might look like, what the needs are. What really is apparent in countries where they have digital literacy as a pillar in their national strategy is this notion that it's not just government led, it's not industry led, it's not just community led, that you really do have to bring multiple stakeholders together to work together.

Mr. Matthew Johnson: Another point where it is relevant is that educating young people is only half the job. The other half is educating parents and grandparents and the general public. That's definitely a role the federal government can play.

Our own research showed that one of the reasons parents and young people both tended to accept the idea of surveillance—even though young people were doing a lot of things to escape surveillance, they accepted the idea that they would be subject to it—was they all subscribed to a number of inaccurate notions about online risks. There was still a sense, even though this has been thoroughly debunked by research, that anyone online is constantly subject to the risk of assault by online predators.

Parents told us they felt a pressure to spy on their kids. If young people are being spied on by their parents, if they grow up their whole lives being spied on by their parents, by their schools, they're going to accept this as normal and they're not going to question corporate or other forms of surveillance. They're going to come to believe that surveillance is normal, and rather than use above-ground tools, the tools that are effective, they're going to use a variety of other tools that are less effective—and we know a few of them from our research—to try to subvert this surveillance rather than control their information.

[*Translation*]

The Chair: Unfortunately, Mrs. Davidson's time is up.

We will now turn to the Hon. Geoff Regan for seven minutes.

Hon. Geoff Regan (Halifax West, Lib.): Thank you very much, Mr. Chair.

[*English*]

Professor Bennett, could you give us some examples? For instance, if you look at what's happening during the American election or if you look at examples from Canada, what are some things that you find troubling?

Dr. Colin Bennett: This is a question to be asking, yes.

One of the things that is currently occurring in the U.S. election cycle is the integration of different forms of data from different sources. The availability of personal data in the U.S. is far more extensive than it is here. The integration of marketing data, geodemographic data, as well as the tracking of online behaviour, is becoming very extensive. It has allowed American political parties in a far more sophisticated way than before to segment the electorate, to divide up the electorate, and to target supporters and potential supporters according to increasingly precise demographic characteristics.

On the face of it, there's nothing in principle wrong with that, but the United States doesn't have any privacy protection rules anywhere near as strong as those in Canada. Yet in Canada, we have seen that political parties here have learned from time to time from their American counterparts.

I would raise the question about whether or not what has been going on in the U.S. might be seen here in the future and whether those kinds of practices are going to raise the concerns of Canadian citizens to the extent that it will be a far more high-profile issue than it is at the moment.

● (1610)

Hon. Geoff Regan: I'd like you to describe why those activities give you concern. Could you specify, for instance, in detail which of those most concern you and what it is about them that concerns you?

Dr. Colin Bennett: There's the lack of transparency. There's the use of tracking devices on websites, spyware that links personal characteristics and personal browsing behaviours to other features. Our privacy protection rules are based on a notion of transparency, consent, and notification when information is being captured about you.

As I've said, there are very few rules that apply in the U.S. Those kinds of practices challenge the basic notion that underpins the kind of privacy protection rules that underpin PIPEDA in Canada, and which suggest that when information is collected about you, you know who is collecting that information, what information it is, and the purposes for which it's going to be used. You have a right to see that information and to correct it if it's inaccurate. You have a right to control to whom that information is communicated.

Those fair information principles underpin our federal and provincial and public and private sector laws in Canada.

It is the lack of transparency, to answer your question more directly, that I think is the most troubling.

Hon. Geoff Regan: Would you make any distinction or draw the line in a different place when it comes to activities designed to get out the vote as opposed to activities designed to convert?

Mr. Brad Butt (Mississauga—Streetsville, CPC): A point of order, Mr. Chair. I know Mr. Regan is new to the committee today. He's visiting. This is a study on privacy and social media. It's not about political parties gathering votes or dealing with information or their own systems. This committee's done a really good job, I think, of having an excellent discussion on privacy and social media. I know Mr. Bennett is a guest, and I let him go on for quite some time in his testimony about political parties, but that is not what this is about.

I would ask you to direct Mr. Regan back to general issues around privacy and social media and not about voting, elections, and all that. It is not relevant to the study that we are doing.

[*Translation*]

The Chair: Thank you, Mr. Butt.

Do you have an answer, Mr. Regan?

Hon. Geoff Regan: If you need an answer, I will say that I do not think this is a point of order.

[*English*]

Clearly this is related to issues of privacy and media. This is why the professor is here as the guest of the committee. If you're looking at the use of social media to collect information, why exclude political parties from that discussion? If you were going to exclude political parties from that discussion, why invite this witness?

[*Translation*]

The Chair: Thank you for your comments. This is not really a point of order but I appreciate your comments.

It is certainly better to stick to social media or to the subject matter of the study we are undertaking according to the committee's agenda for today. So it would be appreciated if members focused their comments as much as possible on social media.

Please, go on.

[*English*]

Hon. Geoff Regan: In relation, professor, to the use of social media in particular, would you like to answer my question?

Dr. Colin Bennett: Yes, of course.

Political parties use social networking. Political parties use social media. Political parties use social media in order to communicate with potential voters, donors, etc., but through that communication they are able to capture vast amounts of information about the individuals.

To clarify, I am certainly willing to speak more generally about the issue of social media and privacy. I have done other work on this. However, when I decided what to speak about here, I thought it was an opportunity to raise this issue, as I had done a study for the Privacy Commissioner of Canada on that question, and the issue of social networking and social media features prominently in that analysis.

I understand what you're saying, and I'm willing to answer any question about this issue. I'm also willing to answer questions more broadly about the subject of your committee, about Facebook, about Google, and about the issues concerning the protection of privacy more generally.

● (1615)

Hon. Geoff Regan: Thank you very much.

Ms. Tallim, you mentioned a group that has a national campaign that anyone can access and use. What struck me about it is that it's great for those parents who are looking for things to access or teachers looking for materials to help children or young people understand the issues at hand, but it doesn't necessarily offer it, in a sense, to that young person.

What else do we need to do to ensure that kids become aware of these issues? How do you ensure that it happens in classrooms and in homes across the country?

Ms. Jane Tallim: You've touched both elements. As we said, a comprehensive approach has a public education direction as well as school-based education.

To deal for a moment with the public education agenda, Go ON UK is just one example of a program that's intended to educate the general population. There are all sorts of support mechanisms within it to facilitate the general public in various community hubs, etc.

Canada actually had an excellent network for this type of public education through the community access program, which was disbanded in April this year. It's a bit of a shame because we had an excellent infrastructure that was already very engaged in the community. You didn't have to push out too much; people knew they were there and could go for education, instruction, help. They were particularly good at reaching a more vulnerable population as well.

Having those hubs is very important to the public education agenda. Consistency and leadership within the schools is also important, making sure, for example, that this education starts in the early years. There are provinces that certainly have outcomes and expectations for privacy education in their curricula, but they don't start until secondary school, and we all know that kids are online far before they hit middle school.

Having that consistency, having a framework that is pedagogically sound and is evidence based would be very helpful, and then supporting it with the necessary training for our educators.

Hon. Geoff Regan: Was it—

[*Translation*]

The Chair: Unfortunately, Mr. Regan, your time is up.

Mr. Carmichael, please.

Mr. John Carmichael (Don Valley West, CPC): Thank you, Mr. Chair.

[*English*]

Thank you to our witnesses.

I too come from the grandparent wing of our table today, so let me start there. Ms. Tallim, maybe you could help me for context. Your associate spoke about grades 4 to 11. Do you have any grounding younger than that, within MediaSmarts?

Ms. Jane Tallim: Yes.

Mr. Matthew Johnson: Just to clarify, it's our research that is studying grades 4 to 11. There are a number of reasons for this. One is so that we can compare data with earlier surveys that covered that age range. But our resources cover the full K to 12 curriculum.

We've made an effort in the last few years to produce more digital literacy resources for younger children, because we know that young people are going online earlier and earlier. It's particularly true with the introduction of touch screen tablets, which are very kid-friendly. It's not at all unusual these days for parents to report that their kids are going online for the first time at the age of two.

We also know from our own research and research done around the world that the landscape online for young people is tremendously commercialized; that the majority of the sites most popular with young people are commercial sites. So it's really important that they develop these digital literacy skills as early as possible.

Mr. John Carmichael: Thank you.

To your point, I have watched grandchildren three, four, and five years old use their parents' iPads and navigate their way through various screens online. It's remarkable to watch. I'm guessing that from a digital literacy perspective, that generation is going to be far advanced, compared even with those who are just a generation ahead, in understanding how the technology works and in being able to navigate it.

The concern I have is the privacy issue. You talked earlier about some examples of best practices, whereby you can go through the privacy regs and accept, be it on a BlackBerry or whatever, the regulations as they exist. Kids at that young age have no idea of that. The concern is, how do you manage it? How do you monitor and control it so that the children aren't getting exposed to things and finding their way into things that they shouldn't be at extremely young ages? It goes from there.

I listened to you talk about the British and Australian models. Could you give us just a thumbnail on how it is that those are such good systems? Is there something there we should be looking to adopt?

● (1620)

Ms. Jane Tallim: I will start with the obvious. Considerable funding has been dedicated in these countries to promoting a digital agenda that facilitates digital literacy skills development. It's largely to—

Mr. John Carmichael: Do you have any idea of the scale?

Ms. Jane Tallim: Oh, my gosh. In Australia, I believe it's hundreds of millions of dollars just for the digital literacy pillar. It's on top of their digital economy plan. You also have quality places created for children online as part of the strategy for children to learn and develop skills.

You were talking about really young children going online, and how on earth they can understand what they're being exposed to. That's where supporting parents and grandparents and adults who are in kids' lives becomes essential in helping people in the general public understand what constitutes a quality website for a child. We all understand that minimal information is needed for a child to participate in online environments. Therefore, understanding exactly what is needed in order to be able to say that a site is respectful of the children who are coming to it is part of that broader education piece, so that adults feel comfortable taking their children to these various web environments.

Mr. John Carmichael: Right. Okay.

Mr. Matthew Johnson: I'd like to add to that.

It's important to know as well that when young people go online, not only are they subject to the same privacy risks as adults, but they're actually subject to greater risks. We know from research done around the world that young people are tracked online more aggressively than adults.

For instance, a *Wall Street Journal* investigation found that on average, children's websites had 30% more tracking devices than adult websites. Similarly, a Federal Trade Commission study was done that looked at 400 mobile apps aimed at kids, and of course these, as we said, are on the devices most popular among younger children, things such as the iPhone or the iPad. They found that fewer than one in fifty actually said what personal information was being collected or how it was being used.

There is really aggressive tracking of kids. There is really aggressive commercial targeting of kids, more than adults are suffering. As you say, they have tremendous difficulties understanding what they are consenting to, if indeed it is possible for children to consent in those situations.

Mr. John Carmichael: When we talk about privacy legislation, and our Privacy Commissioner is well regarded for the work that's been accomplished to date, do you believe that stronger enforcement powers are needed to make sure companies respect privacy legislation? Should she be given more authority in her role to ensure that in the event a company transgresses, she would have the authority, some teeth in taking control of a situation, be it monetary or however it is weighed?

Ms. Jane Tallim: The Privacy Commissioner would be better positioned to specifically address whether she feels she has sufficient power to work with companies. Certainly having these standards, whether they are entrenched in legislation, or whether it is decided that these should be self-regulatory codes and guidelines, as has been done in other media, when these standards are put out, they do become the benchmark. They become the bar that companies are expected to reach one way or another.

● (1625)

Mr. John Carmichael: We have asked her, and—

[*Translation*]

The Chair: Please ask your question very quickly.

[*English*]

Mr. John Carmichael: Time flies. My apologies.

[*Translation*]

The Chair: I want to remind you that you should not touch the buttons on your microphone. We have experts who are here specifically to take care of that. They will do it for you.

Do you have something to add? Nothing?

[*English*]

Mr. John Carmichael: Was my time up?

The Chair: Yes.

Mr. John Carmichael: Oh, it was.

[*Translation*]

The Chair: However, the witnesses can answer if they have something to add.

[*English*]

Mr. Matthew Johnson: I will add very briefly that whatever regulation or legislation takes place, it is really important that the education piece be there, to make sure young people are aware of the rights they have under legislation or regulation.

Research has shown that a large proportion of young people in the United States believes the law in that country protects their privacy more than it actually does. There is definitely an inaccurate sense among young people of how much they are protected.

We don't know whether that's true in Canada yet, but there's every reason to believe that it is.

[*Translation*]

The Chair: Thank you.

We will now start a new five-minute round.

Monsieur Boulerice, you have the floor.

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Thank you very much, Mr. Chair.

I also want to thank our guests for being with us. We do appreciate it.

I am a privileged witness because I can tell you in fact that a two-year toddler can navigate on an iPad and choose the videos he wants to watch on YouTube. He does. He knows he can play a video by touching the arrow icon and pause it with the two-bar icon. I understand this can be a cause for concern.

My first question is to Professor Bennett.

Dr. Bennett, you are working on a research project entitled "The New Transparency: Surveillance and Social Sorting." Can you tell us about your findings? How can you reconcile the social networks and social media environments with what I would call our reasonable expectations regarding respect for our privacy? What is your assessment of the present situation?

[*English*]

Dr. Colin Bennett: Thank you for your question.

The project has centred at Queen's University and we're looking at various trends in surveillance that have occurred over the last 10 or 15 years or so. There are several things that we would point to.

First, there is the fact that surveillance has become more mobile. It's become more general. It's not just about who you are; it's about where you are.

Surveillance has become more embedded in material objects. We don't necessarily know that we're being watched. Surveillance is also something that is not just done between big organizations and individuals. It's also something that happens from peer to peer.

There are a variety of trends that are occurring, and social networking and social media are central to all of those trends. That's why I have difficulty saying that social media and social networking are things that are out there, things that big corporations do. They are deeply embedded in all of our organizations.

With respect to privacy, it is true that our privacy protection rules need to be considered and updated in relation to social media, and particularly with respect to this issue. Our laws, such as the Privacy Act and PIPEDA, were developed with the notion of a distinction in mind between an organization and a subject, or between a controller of data and an individual. Now that distinction has broken down as social media sites are producing and selling data that is actually generated by users. It's that notion of user-generated data that really does challenge some of the existing principles within our privacy protection laws.

I want to say something in response to the previous question about enforcement powers.

The Privacy Commissioner of Canada has ombudsman powers. I am in favour of broader enforcement powers. They're certainly necessary in the light of these rapid changes in technology. More enforcement powers would create a greater certainty for consumers and indeed for businesses.

It would establish a clearer jurisprudence where the rules and the investigation reports would have a clearer legal standing than they perhaps do at the moment. It's also a little odd that some of our provincial commissioners, such as in Quebec, British Columbia, and Alberta, do in fact have enforcement powers under their respective privacy laws, when the Privacy Commissioner does not.

● (1630)

[*Translation*]

Mr. Alexandre Boulerice: Dr. Bennett, I have to interrupt you because I only have five minutes. I can now see why it may be risky to ask a university professor to give an assessment of the situation.

While preparing for today's meeting, I learned about new facial recognition technologies that can be used by people who design billboards for shopping centers or grocery stores. Using these technologies, it is possible to determine if the person looking at the billboard is young or old, male or female and so on, so the ad can be adapted to that person. According to the articles I read, it would even be possible to link this to information and pictures that may exist in this person's Facebook account. It would be possible to identify the person and all related information: children, income, address, etc.

Don't you think this is somewhat disturbing? I do. What do you think of the possibility of using facial recognition to link social media information to direct advertising?

[*English*]

Dr. Colin Bennett: It is a deep concern, as companies such as Facebook and Google are increasingly using facial recognition. The ability to identify somebody more precisely from simply taking a picture of them is something that should be of concern to all of us. It would encourage greater stalking, cyber-stalking and other stalking. More broadly, I think it raises another trend that I was alluding to, that the distinction between personal information and non-personal information is becoming increasingly difficult to identify.

We tend not to think about personal information anymore, or personally identifiable information, but whether it is personally identifiable information, and facial recognition, the ability to link up a face or an image to a real individual is an example of the increasing identifiability of all of us online.

[*Translation*]

The Chair: Thank you very much.

We will now turn to Mr. Dreeshen for five minutes.

[*English*]

Mr. Earl Dreeshen (Red Deer, CPC): Thank you to our witnesses.

I'm a former high school teacher. I taught school for 34 years.

My daughter actually teaches an educational technology course out of the University of Alberta, where she teaches online to teachers who will end up teaching in an online platform. The education industry will have to be aware of how these types of things are happening in the future, so it's how you do the training and everything else.

I noted, from your digital literacy discussion, that those types of things are needed for the students, but also at the educational level, at the teaching level, with the opportunity perhaps to go to teachers' conventions and those types of things. They're great opportunities for awareness, certainly.

I have a question about something you mentioned earlier. It's the concern that students realize they're being watched at school, and realize they're being watched at home, and therefore don't see their privacy as being something that they have any control over. Of course, if they get into sites on school time and in a school setting, you know what kind of difficulty would occur there, so they have to be able to protect themselves. I'm wondering if you have looked at how that can all be done.

As well, when you talk about digital literacy, I'm wondering if you're also explaining to them that this isn't a free service, and that the reason it's out there is for these industries to be able to gather information, which I think sometimes we forget.

I'm wondering if you could comment on that.

Ms. Jane Tallim: Sure. I'll start, and then I know Matthew will have lots to say.

I think one of the issues you mentioned is that training is so germane. Professional development training is almost going the way of the dodo bird. I believe at the Ottawa Board of Education there are currently two professional development days a year, and there are teachers who are teaching many different subjects, as well.

I also think our faculties of education are struggling to keep up with the whole change in education at all the levels you alluded to. We need to better train our teachers to teach through technology and teach about technology.

● (1635)

Mr. Matthew Johnson: Absolutely.

A study was done just last year with pre-service teachers, or teacher candidates, in Ontario. They said overwhelmingly that they did not feel they were being prepared to deal with the various digital issues they were going to face in the classroom. One of the ones they touched on was cyber-bullying, which is top of mind for many people. That too has a privacy dimension, because much of cyber-bullying does relate to unethical use of other people's privacy and personal information, their images, for instance, in many cases.

That's one of the reasons we have to address privacy. It's from a perspective of not only protecting your own personal information but also dealing with privacy in an ethical way. That relates to the corporate collection of privacy, because if we inculcate young people with the idea that privacy has an ethical dimension, they'll expect and indeed demand that their personal information be treated ethically by the spaces, the corporations, to whom they give it.

Mr. Earl Dreeshen: There was also discussion about the amount of information that was gathered on young people. One of the things we heard was that perhaps there should be a way that, at a certain age or whatever, you could delete all of that type of data.

We're trying to talk about policies, and to look at different types of things, so I'm wondering if you could make a comment.

Ms. Jane Tallim: Certainly.

The education piece fits squarely into that. When you're looking at data retention, you're looking at corporate responsibility, being amenable to removing images and data at a certain point.

The education piece is really important, though, especially with youth. You could have a company that is very respectful of this, that doesn't retain profiles after a certain time period after they're closed. However, if a young person, or anyone, has been indiscreet in over-sharing photos, texts, or anything like that, these images and texts have a life of their own beyond the courtesy of the company where those were posted.

It's a double issue there. The education piece is central in just thinking about what you post online, especially for youth.

[*Translation*]

The Chair: Thank you, Mr. Dreeshen. Unfortunately, your time is up.

Mrs. Sims, please. You have five minutes.

[*English*]

Ms. Jinny Jogindera Sims (Newton—North Delta, NDP): Thank you very much. It's a pleasure to be here.

I'm glad to be here talking about one of my favourite topics, digital literacy, being a Luddite when it comes to this and having grandchildren who know far more than I do about all of it.

This is a topic that's close to my heart as a teacher. As you may know, I was on the Canadian Teachers' Federation executive for a number of years and on their board of directors. This issue has been a great concern to the teaching profession right across the country. They have been calling on governments at all levels to do more in this area, both in the teacher training aspect of it, but also in providing resources, by way of curriculum and tools that can be used in the schools, as well as by doing some pre-school work with parents. We know how challenging this can be.

It's always great to have somebody here from my home province, and from Victoria, one of my favourite cities.

My first question is for Matthew and Jane; either of you can answer it.

How has the elimination of the community access program impacted access to digital literacy training in Canada?

I'm specifically interested in a comment you made in which you talked about Australia and the U.K. taking this issue a little more seriously than we do. Could you explain what drove that comment from you? Are we providing enough resources as a federal government to ensure that we have the kind of literacy we need for our youth?

● (1640)

Ms. Jane Tallim: Thank you for your question.

I'll bring it even closer to home. An initiative in the United States is a digital literacy corps of young people who are trained to go out into the community and provide training to members of communities in various cities across the country.

Looking at these and other initiatives, we found it sad that we have an excellent system set up that is very well respected, that is doing good work, that is reaching those people who might be more difficult to reach, and that we denied it funding. It's sad because at the end of the day we're going to have to go back and reinvent the wheel, and we'll probably come up with another CAP system, when we actually have systems that are invested in communities and are well respected and are doing good work in communities.

Ms. Jinny Jogindera Sims: Absolutely I'm hearing from you that you're looking to parliamentarians, those of us around this table and in the House, to ensure that we provide adequate funding so that we do not fall behind other countries that are doing such a great job in this area.

Ms. Jane Tallim: Yes.

Ms. Jinny Jogindera Sims: As you said, it's a very complex matter. It's multi-faceted, and there are no easy answers. Yet we have to start somewhere, and the community access program, I know, was certainly one stepping stone.

Thank you very much for that clarification.

My next question is for you, Colin. In one of your recent presentations on the geopolitics of personal data and the governance of privacy, you have undertaken substantial research into privacy issues, not just domestically but internationally.

In your presentation you discuss trends in surveillance practices. Could you elaborate on some of those trends? I'm trying to get a sense of some of them.

Let me also mention that, as you know, at our border we're moving more towards biometric data collection as well. What do you see as some of the concerns in that area?

Dr. Colin Bennett: I will continue on with the trends. The collection of biometrics at the border is something which the Privacy Commissioner has expressed a great deal of concern about.

It depends a bit on what you mean by a biometric. That's a word that's not used consistently, but it speaks to my broader points. The nature of information is changing and the ability to monitor people is changing as a result of changes in the way we think about identifying people.

Perhaps I could add something historically to emphasize my point.

There was a time, maybe 30 or 40 years ago, when we knew when information was being captured about us because we filled out a form. We were asked for a certain amount of information and we filled our a census form or an application form, or something like that. Now, increasingly, we do not know when that is happening. Furthermore, we don't necessarily know the nature of the information itself. We don't know how we are being identified. One of the larger trends, in addition to those that I mentioned earlier, is that we don't know, as individuals, how organizations are actually identifying us. We don't know how that happens online, and we certainly don't know how it's happening with respect to biometrics. Yet our laws tend to be based on a fairly dated notion of what personal information is and is not, and it's creating challenges for the Privacy Commissioner here and for her colleagues internationally.

I hope that h as addressed part of your question, at any rate.

Ms. Jinny Jogindera Sims: Thank you very much.

[*Translation*]

The Chair: Mrs. Sims, unfortunately, your time has expired. I would have loved to hear more of this but I have to interrupt you because we must go to the next point on our agenda.

I wish to thank our distinguished guests who have taken the time to come today to explain their points of view to the committee.

As we did at our last meeting, we will have to update the witness list. Since the list is not public, we have to sit in camera to update it.

Once more, thank you very much.

Members, we will resume in a few minutes.

[*Proceedings continue in camera.*]

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