HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 068 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, September 25, 2017

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Monday, September 25, 2017

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I call the meeting to order.

Welcome, everyone, to the Standing Committee on Access to Information, Privacy and Ethics. Today we're continuing to study PIPEDA, as we all know it, the Personal Information Protection and Electronic Documents Act.

We'll start off with Jane Bailey.

You have 10 minutes.

Professor Jane Bailey (Professor, Faculty of Law, University of Ottawa, As an Individual): Thank you.

Together with Professor Valerie Steeves, I co-lead a seven-year project funded by SSHRC called the eQuality project. It's focused on understanding how big data practices, especially targeted advertising, affect young people's online interactions and can set them up for conflict and discrimination.

Today, I'm going to be drawing from research from several Canadian studies on young people. Two are 2017 studies. One was conducted by the eQuality project for the Law Commission of Ontario and is related to online defamation. The other was co-conducted by the eQuality project and MediaSmarts, under a grant from the OPC. It focused on young people's decision-making about privacy in the context of posting photos online. I'll also draw from the eGirls project, which was a three-year project co-led by Professor Steeves and I that looked specifically at young women's and girls' online experiences. Finally, I'll draw from the results of the MediaSmarts study entitled “Young Canadians in a Wired World”, most recently reported on in 2015-16.

Basically, I think there are three take-aways from these studies of relevance to this committee. First of all, young people are very concerned about reputational harm, and for girls and young women in particular, permanent reputational harm is considered by many to be the danger associated with networked media. Second, privacy, particularly the mechanisms for controlling access to and use of young people’s data is foundational to addressing these harms, particularly as young people think about whether and how the information they post or that is posted about them now may be unfairly used out of context in the future in ways that interfere with their prospects for employment and maintaining healthy relationships, among other things. Third, young people do have strategies and norms to mitigate these dangers, but corporate practices and online architectures make it very difficult for them to implement those strategies, or invisibly undermine them through machine-based processes such as algorithmic profiling for targeted advertising.

In a nutshell, from the studies on youth perspectives from our Canadian research, young people do actively seek out online publicity, but they are also particularly aware of the complications that publicity introduces. Because of this, they rely on a number of strategies to protect their online reputations, including thinking very carefully about what they post, monitoring what other people are posting about them, and getting colleagues to assist them when material is posted about them that is negative. However, the commercial nature of networked media makes it very difficult for them to keep control over their reputations.

In what we've come to call a perfect storm, digital architectures incent young people to shed data that is in turn used to profile and categorize them for purposes of targeted advertising. This involves predictions about who they are and who they ought to be that are often premised on narrow, mediatized stereotypes and presumptions about the groups into which they are aggregated. When young people try to reproduce these stereotypes themselves in order to attract the “likes” and “friends” set up by platforms as numeric markers of success, they are opened up to conflict with others who monitor, judge, and sometimes stalk them.

In this environment, we asked young people what policy-makers should do. I have four things I want to share with you.

The first thing is that you need to directly engage young people in the policy-making process. Policy development models need to be reformed to require direct engagement by young people from diverse social locations as experts in the policy formulation process itself, because research to date indicates a serious gap between policies set by adults and the experiences of young people.

Second, we need to look for responses that go beyond telling youth what to do and what not to do. The young people in the research that I'm drawing from today understood that being involved in networked spaces was essential to their lives, and all indications of our social, economic, and cultural worlds affirm that reality. It's not just an impression that they have. In fact, we’ve spent billions of dollars and years of policy and program development trying to get them online and to keep them online as part of our economic development plans. As such, advice like just going offline if you want to protect your privacy or you don't want to be harassed is both unrealistic and insulting.

● (1535)

Third, move beyond informed consent models. In the current environment of surveillance and prediction that is largely invisible to the user, traditional data protection models based on consent just aren't enough to protect young people's privacy and equality because, in many cases, no one can even explain what it is that machines are doing with our data. Further, and in any event, if we could explain that, simple disclosure of those processes wouldn't be enough because network technologies are so embedded in young people's lives that young people really have no choice but to consent to terms of use that purport to allow these practices, even when they don't agree with or understand them.

Fourth, we need to regulate platform providers to improve privacy and equality. Many of our participants suggested that platform providers should not be permitted to keep young people's data as long as they do. This was in part because they were so conscious of how the permanent cache of information about them opened them up to judgment and reputational harm that could affect them now and in the future.

There are a number of potentially responsive regulatory options. First of all, as many people have testified before this committee, we can ensure that the OPC has enforcement powers in order to deal with these issues effectively.

Second, we can mandate greater accountability and transparency by service providers as a first step to better understand what exactly it is they are doing with our data to profile us and shape our online experiences, and to find out how often that profiling and those processes are premised on discriminatory stereotypes or yield discriminatory outcomes that affect individuals' life chances.

This kind of profiling—machine-based, invisible to users, involving processes humans often cannot understand or explain—can lead to discrimination on grounds that are currently legally prohibited, some of which could have serious implications for young people in particular. Currently, it's very difficult to open up the black box and understand exactly what it is that's happening, although we get glimmers from research projects such as that of ProPublica, which recently revealed discrimination in the price of SAT prep tests such that Asian students were more than twice as likely to pay a higher price for a prep test because they were Asian or because they lived in a zip code that was associated with Asians from both high- and low-income groups. It may well be that insights gained from this kind of disclosure from service providers about what it is they are doing will make it even clearer that the best option is just to prohibit the use of young people's data for the purposes of targeted advertising, full stop.

Third, we can consider legislative provisions that are better aimed at supporting young people in protecting their reputations now and in the future than the current PIPEDA provisions relating to accuracy and completeness. These include examples such as the right of erasure, as seen in California, and the right to be forgotten, as seen in the European Union, which I can say more about if others are interested later on.

Finally, if we're simply too wed to the consent model to depart from it despite knowing its obvious limitations in the climate we're in, we could consider requiring service providers, regardless of their terms of service, to get separate, explicit consent from young people or their parents to use their personal information for targeted advertising, and to provide ongoing, easy opportunities to opt out of that decision. It's less likely to be as effective as any of the other things I've talked about, but at least it offers the possibility of interrupting the commercial cycle of presumed access to young people's data.

In conclusion, the current commercial “data for services” model of network communications renders young people vulnerable to discriminatory profiling and reputational harm that can have long-lasting impacts. It's time for us as adults to take responsibility for the economic and social policies that have resulted in their seamlessly integrated online-offline world. Carrying out that responsibility requires the direct engagement of young people from a variety of social locations in processes like these, rather than just asking for the opinions of adults like me who have had the privilege of working with some of them.

Thank you.

The Chair: Next, we have Mr. Owen Charters and Ms. Rachel Gouin from the Boys and Girls Clubs of Canada.

I'm not sure which of you is speaking, or both, so please go ahead. You have 10 minutes.

● (1540)

Mr. Owen Charters (President and Chief Executive Officer, Boys and Girls Clubs of Canada): Thank you, Mr. Chair.

I'd like to thank the committee for inviting us to be here. I'm the president and CEO of the Boys and Girls Clubs of Canada. Rachel is our director of research and public policy. We're excited to be here to present as part of the study on PIPEDA. We're pleased, actually, that the committee is spending some additional time, especially on this issue of children's privacy. We've shared our full recommendations in a letter already, but I want to go into a little more detail today.

One of the things you should know is that the Boys and Girls Clubs of Canada is Canada's largest child and youth serving organization. We serve about 200,000 children and youth across the country in more than 700 locations. We're there during the critical out of school hours for children. Our clubs offer children safe spaces. They can explore their interests, develop their strengths, and realize positive outcomes in terms of self-expression and academics. We do all sorts of programs around healthy living, recreation, mental health, and more. Our trained staff and volunteers help young people build the confidence and sense of belonging that they need to overcome barriers, form positive relationships, and mature into responsible, caring adults.

What is really important is that we offer a range of programs that are focused on education, digital literacy, and coding. Many of our clubs have tech centres that facilitate children and teens' access to the Internet. We are often enabling young people's access to online environments, especially if they don't have have access in many other places. Part of that is what brings us here today.

While we're doing our part to equip Canada's young people with digital and media literacy skills to help them navigate the online environment, we are concerned that marketers are collecting private information from minors, without meaningful consent. We're here to ask the government to explicitly include children's privacy rights in the Personal Information Protection and Electronic Documents Act.

We think that's important for two main reasons. One, from a developmental perspective, young children are not able to properly determine the risks associated with sharing private information online. Media skills training is definitely not enough in that regard. Two, we recognize that children are online at a young age, and sharing personal information for years before they reach the age of majority. We know that corporations are compiling quite a profile of Canada's children, and we don't think that's right.

While guidelines do exist, we know for instance the Canadian Marketing Association has a code of ethics, and the Privacy Commissioner has also issued guidelines. However, the collection of children's private information by corporations is not regulated or enforced.

In 2015, the Office of the Privacy Commissioner participated in a global sweep that determined that many websites and developers were failing to adequately protect children's privacy. In Canada, that amounted to 62% of those who reported. We discovered that they may disclose personal information to third parties, and that is simply unacceptable.

Last February, we published an op-ed calling on the government to introduce a law that would protect children's online privacy. Such a law does exist in the U.S. The Children’s Online Privacy Protection Act, or COPPA, requires parental consent for collecting personal information from children under 13. We want to add our voice to those calling on the government to explicitly include children's privacy rights in PIPEDA.

Today we're asking for four measures to be undertaken.

First, we ask the government to prohibit the collection, use, and disclosure of all personal information from children under the age of 13. Children are accessing the Internet at younger and younger ages, and from their own personal devices. They're too young to understand the implications of data collection and use. There need to be limits on what is appropriate to be collected, and restrictions on the types of data that can be collected from websites and applications aimed at children. I, personally, have often noticed that my own children have wandered away from the website, or the application I have opened for them, and may be attempting to visit new sites. Clicking on surveys and answering questions is a game for them, and does not come with an understanding that this is trading personal information for access.

The second recommendation is that the government follow the lead of the European Union's general data protection regulation, and require parental or guardian consent for access to online services for children aged 16 and under, or as that particular guideline requires, a lower age but no lower than 13. It is important, we feel, that parents be involved, as only parents or guardians should be able to provide informed and explicit consent for the collection of information. Parents should be aware, and responsible for the activities of their children online, and mechanisms that require explicit parental consent also serve to ensure engagement and awareness of what children are visiting and exploring online.

We were particularly struck by Dr. Valerie Steeves' February 16 testimony. I know she is a colleague of Madam Bailey. She found that almost none of the 13- to 16-year-olds she surveyed could remember the point at which they consented to the collection of their information when they signed up or posted material on Snapchat or Instagram. When we also consider Dr. Steeves' finding that 95% of 10- to 17-year-olds surveyed said that marketers should not be able to see what they post on social media platforms, we can conclude that young people's consent is definitely less than informed.

● (1545)

Our third recommendation is that we ask the government to provide children and youth the right to be forgotten when they reach the age of majority, requiring that corporations be obligated to remove private information immediately unless the newly adult person gives his or her explicit consent to the continued collection, use, and possible future disclosure of their personal information gathered during their minority.

We know how children use the Internet, and the choices made while under the age of majority are not reflective of the identity and choices they will make once they have reached the age of majority. While we know there are also many out there who would like their online life to be erasable and forgotten, children should actually be able to benefit from this right.

Lastly, we want to make sure that these new rules are enforceable. We ask the government to give the Office of the Privacy Commissioner the power to enforce new children's privacy regulations. It is not enough to just create these laws. Companies and sites must be monitored and held accountable for their compliance with these provisions.

Some have argued that there are jurisdictional issues in overseeing consumer rights and that this might be a provincial issue. However, we would encourage two particular perspectives on this. First, the federal government needs to show leadership in this respect. The laws in the U.S. governing children's protection date from 1998. We are sorely behind in this regard, almost 20 years, which is an entire generation of children growing up on the Internet in this unregulated environment. Second, we'd argue that this is not about consumers, as children are not the purchasers in a household, but about protection and privacy of children's personal information.

Education is as critical as enforcement. Resources such as those that have been developed by the Privacy Commissioner, those that have been developed by MediaSmarts, as mentioned already, and those in the U.S. such as “Stop, Think, Connect”, from the National Cyber Security Alliance, need to be promulgated to Canadian families and educators and make sure that Canadian resources are further developed for use.

Some have commented that it is unusual for a general youth-serving organization such as ours, the Boys and Girls Clubs, to choose to advocate for the protection of children's privacy rights. However, we're proud to stand up for children and youth on a broad range of issues. We were conducting background research on Internet safety and were actually, frankly, surprised by the lack of protections for children in Canada. We are concerned about Internet access, and children are accessing the Internet more frequently, often within our clubs and our technology centres and on their own devices.

The review of PIPEDA offers an opportunity for the government to address that gap. Boys and Girls Clubs of Canada is proud to add our voice to this mix, and we're grateful for the opportunity to speak about the privacy rights of Canada's children and thank the committee for taking additional time to address concerns specific to this population.

We hope that the discussion will lead to stronger protections for children, protections that can be best asserted by explicitly including children's privacy rights in PIPEDA. We will welcome your questions.

The Chair: Thank you, Mr. Charters.

Next we have the National Association for Information Destruction, Canada. Mr. Backman, you have 10 minutes.

Mr. Kristjan Backman (Chair, National Association for Information Destruction - Canada): Good afternoon, and thank you for the opportunity to be here today.

My name is Kristjan Backman. I chair the National Association for Information Destruction in Canada. This is a voluntary position. In my day job I run a small company called Phoenix Recycling. We're a Winnipeg-based company that does information destruction services.

NAID-Canada is a non-profit association representing companies that specialize in the secure destruction of information, with members in every province across Canada. Our mission is to raise awareness and understanding of the importance of secure information destruction, and in doing so we want to ensure that private, personal, and business information is not used for purposes other than for which it was originally intended.

NAID-Canada also plays an active role in the development and implementation of industry standards and certification. We provide a range of member services, which include advocacy, communication, education, and professional development. It's worth noting that NAID certification is often mandated contractually by clients who use information destruction services to ensure that service providers meet regulatory and security requirements.

The issue I'm here to address today is often overlooked, yet is a critical aspect of privacy protection, namely the secure destruction and disposal of records that are no longer needed. Our mantra in NAID is that information is only as secure as the weakest link in its life cycle, and far too often little attention is paid to the end of a document's life cycle. We see evidence of this on almost a daily basis in the media, with reports of information being left intact and publicly accessible in dumpsters, recycling bins, and discarded electronic devices sent for reuse and recycling.

It's difficult to measure how pervasive this problem is, but NAID-Canada and our sister associations around the world have conducted investigations into unsafe destruction practices. Our first such investigation was in Toronto, in the GTA, in 2010, when NAID hired a private investigator to go dumpster diving and look for personal information. In that survey, 14% of the commercial dumpsters that we examined had personal information intact and easily accessible to the public. That exercise has since been repeated in Australia and Spain and has sparked national conversations in those countries around the failure to securely destroy information that's no longer needed.

As the world becomes increasingly paperless, the threat of unsafe destruction of information has become more complex. All the electronic devices that we store information on, and wiping those devices of that information when disposed of, has become a major privacy issue. As evidence of that, in April our U.S. association released the results of the largest-ever study looking for the presence of personally identifiable information on electronic devices sold in the second-hand market. It found an astonishing 40% of the devices sold through publicly available channels contained personally identifiable information. These are tablets, cellphones, PDAs, and hard drives.

I know the committee is interested in youth privacy protection, and there is perhaps no demographic more impacted by a failure to securely destroy information stored on electronic devices. The implications for anyone having their entire private life exposed if personal electronic records are breached is severe, but for youth more so. We recently received a letter from the Privacy Commissioner about a recycled devices study, and we agree with his assessment in this area, where much more education is needed, particularly with youth.

With destruction more generally, we've had many cases in Canada of sensitive personal files, including those related to youth, being breached through a failure to destroy personal information. This has included medical records and client files from the Children's Aid Society. Again such breaches are potentially devastating for all ages, but more so for youth.

This is just a snapshot of the problem. Let me turn to some solutions, which are detailed in our written submission that we made to the committee.

NAID-Canada believes that PIPEDA should include specific requirements that information must be destroyed when it's no longer needed, and that destruction should be defined in the legislation. Currently destruction is only a recommendation in PIPEDA, not an obligation. We believe that making it an obligation would force organizations to treat destruction more seriously. As for a definition, NAID-Canada defines “destruction” as “the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information, or parts thereof, is not practical”. This definition applies both to paper and to electronic records as we believe the specificity of the definition is required in the legislation to ensure “destruction” is not left to interpretation.

● (1550)

Recycling, for example, is not destruction as records may remain intact and vulnerable to a privacy breach for extended periods of time.

Putting a destruction obligation into PIPEDA and defining the term are our two primary recommendations, and I should note that they were endorsed by this committee the last time it reviewed PIPEDA. The government, instead, felt the issue could be addressed with guidelines, and those guidelines have been developed. However, we still believe destruction should have legal weight behind it.

Building on that point, I would note that other jurisdictions impose significant fines for failing to properly destroy information. For example, a Missouri medical company was fined $1.5 million for leaving medical records in a public dumpster. In Canada, we have an epidemic of cases involving medical records in dumpsters. Perhaps we wouldn't if we had proper fines like those in the United States.

NAID Canada supports fining and order-making powers for the Privacy Commissioner. Likewise, we support breach notification laws and look forward to their implementation here.

Finally, please let me close with a general comment about Canada's global standing in privacy protection. As our organization has branches around the world, we have considerable insight into that, albeit from our fairly limited perspective of information destruction. That said, Canada is falling behind. Other countries have been far more decisive in mandating safe information destruction, and the fines in the U.S. are punitive. The long delays in getting breach notification law into effect in Canada put us well behind many of our peers, though we are pleased to have seen the draft legislation to implement this law finally published earlier this month.

Also, we have noted the considerable attention paid during these hearings to the more aggressive general data protection regulation in the EU that will go into effect this year. European policy-makers have learned what all regulators eventually do—that clear, unambiguous direction and strong enforcement provisions are the only way to ensure the protection of personal information.

As we remind the committee, we service providers are subject to the same stronger penalties. Even so, we are willing to confront this increased liability because we realize it's better for everyone, and it's really the only solution.

In closing, let me state that we are sensitive to those who are concerned about compliance costs, and our members are businesses, so we get that. However, any smart business should already be securely destroying the information that's no longer needed since the financial and reputational risks of a breach are far greater than the costs of securely destroying the information.

That said, incidents related to a failure to safely destroy information keep happening, and it has been almost a decade since the last PIPEDA review. We think it's time to amend this legislation to include a secure destruction obligation and a definition of what that entails.

Thank you for your time, and I look forward to your questions.

● (1555)

The Chair: Thank you, Mr. Backman.

Just to note, we're going to be done our meeting today at five o'clock because we have committee business. We have approximately an hour.

We'll start with MP Long for seven minutes.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair.

Thank you so much to our presenters this afternoon. They were very interesting.

I'm going to start with a very quick, broad question to each of you, starting with you, Mr. Backman. Should we just forget about the right to be forgotten? Is it even realistic?

Mr. Kristjan Backman: No, I don't think you should forget about the right to be forgotten. I think that with information being collected and aggregated in ways that we don't understand, I think the ability to say to the people who are collecting that information that they need to get rid of it is important.

Mr. Wayne Long: Ms. Bailey.

Prof. Jane Bailey: Yes, I agree. I think the right to be forgotten is going to become more and more relevant the more complex data collection and profiling systems become.

Mr. Owen Charters: I actually think there's an interesting piece in that question, which asks whether it is actually technically feasible, because we know there are things like the Internet archives that collect and archive pieces.

But I don't think that should prohibit us from attempting to do what I think is important, especially when we're talking from the perspectives of children and youth. Unless you understand the consequences of the information you're posting, I think you need to be making the more-than-valiant effort. I think we need to be doing the right things, ultimately, in order to make sure that there is some semblance of a right to be forgotten enshrined in law.

Then the next piece is how you actually make that take effect, and I think we're seeing that all over, from trying to regulate those who are uber to others, let alone trying to understand how you erase an identity. But I think it's a piece that needs to be enshrined, and then we figure out the “how”.

Mr. Wayne Long: Thank you.

Ms. Bailey, with respect to PIPEDA and meaningful consent, we all see these stats. I think they probably change weekly. Give or take, roughly 75% of youths 13 to 17 years old have cellphones now, 71% use more than Facebook, and 92% are on social media daily.

With respect to meaningful consent, here's what scares me. My kids aren't really kids anymore—they're young adults—but we certainly have friends with younger children. As recently as two weekends ago, we were home and had some of our friends over. Their kids were there and of course were on their cellphones. I took a little more notice of what they were doing. They were going through sites and apps and clicking on agreeing to this and that.

With respect to meaningful consent, especially in Canada with PIPEDA, I'd like you to elaborate a bit on the GDPR and on COPPA in the United States, but what can we do in Canada with respect to tightening up meaningful consent? Is it consent by 17-year-olds and up, as I think one of you mentioned, and you're good to go? For 13 to 17, do you maybe need parental consent?

Can you elaborate on meaningful consent and how you would like to see that tightened up in Canada? Can you compare it with the GDPR and COPPA?

● (1600)

Prof. Jane Bailey: I don't think meaningful consent is real. I don't think you can have informed consent in the environment we're living in, and we won't have it in the future, because meaningful consent is informed consent, and you can't be informed of things you can't understand. The best-intentioned industry players cannot explain things like how the Facebook algorithm decided to allow people to place ads for “Jew haters” as a group. They can't explain that.

Informed consent, then, becomes a very problematic concept. That is why I said all of those other things, and why I said that if you're so wed to informed consent, then I think you have to start thinking about measures that.... The thing about it is that if you say, okay, if they're 13 to 17, we'll have their parents' consent, but their parents won't understand it. I don't understand it. It really isn't isolated to young people. Nobody understands exactly what's happening with their data.

To me, what we have to be thinking about is what we're going to do about regulating the collection, retention, and use of data instead of trying to pretend that we're going to have this individual consent model in a situation where people cannot understand what they're consenting to.

Mr. Wayne Long: I'm going to come back to you, if you don't mind.

Mr. Charters, can you elaborate on what you think with respect to meaningful consent with regard to the Boys and Girls Clubs? What rules do you have in your clubs with respect to social media and youth on cellphones? Can you elaborate on how you think we can tighten up what meaningful consent should be and how we can enforce that?

Mr. Owen Charters: Sure, but I can tell you that we haven't spent the time on getting as in-depth or nuanced a view as my colleague's, which I find quite interesting, because things such as the Equifax hacks concern me. I don't think people knew their data was being used in those ways.

It's exactly that, and we at least are saying that there needs to be consent from someone who at least has the responsibility and the knowledge to try to know better in terms of what those risks might be, hence the parental consent.

Mr. Wayne Long: How do you enforce that?

Mr. Owen Charters: We've seen it on sites, especially for Internet providers that are in compliance. If parental consent is required, there is an email verification, an age check, and a check-in by creating an adult account alongside a youth account, with teacher and educator accounts alongside youth accounts. They're managed through someone who has been verified to some degree. There is obviously no “perfect” in these processes. That's what we've seen in those who are in compliance with COPPA. Some best practices along those lines would be the route to go ultimately.

Mr. Wayne Long: I'm curious. With respect to the Boys and Girls Clubs, what rules do you have in the clubs with respect to children on phones and using social media?

Mr. Owen Charters: Part of that is very club-to-club specific. It can vary, but generally speaking, in most of the clubs, personal devices, especially for young kids, are to be put away while they're in the club.

The use of any other access to the Internet is done under supervision. There are tech centres built into many of our clubs. They're managed under supervision. They're used mostly for the purpose of academics, such as finishing homework or doing a project. They're done with academic mentors in the room who are able to observe what's happening, both on screen but also from a central location. As they get older and into the age brackets where as teenagers they're using personal devices to check in with parents and so on, the rules become a little looser, and there's less that the club will often to do to manage that.

However, again, there are rules where those devices need to be put away. There are times when they're device-free and we're focusing on the activities at hand, which I think is very similar to what you'd see at a school.

Mr. Wayne Long: Sure.

Thank you for your answers.

The Chair: Next up is MP Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair.

Thank you all for sharing your insight and expertise. I'll start with the matter of education. Anecdotally, in Toronto and the GTA, some teachers in some elementary schools have made it part of their grade 1, grade 2, or grade 3 courses before they become formalized, to talk about the responsible use of and participation in online services, games, and so forth.

You mentioned the complications of jurisdictional direction and authority in terms of setting up new regulations, but I wonder whether you would recommend that, in fact, online behaviour and best practices be as much part of the curriculum from the elementary level upwards as reading, writing, and arithmetic.

● (1605)

Mr. Owen Charters: That's interesting. We haven't taken a specific position on that, but I would say, absolutely. We try to provide education to kids of all ages throughout the process, as they become more adept online, and ensure that, just like learning to cross the street safely, this is another environment where that safety needs to be taught from an early age and imbedded in that conversation from the beginning. That's an ongoing conversation.

I would see no reason not to do so. It would make a lot of sense.

Dr. Rachel Gouin (Director, Research and Public Policy, Boys and Girls Clubs of Canada): I think what Ms. Bailey was raising is that the education and the strategies that young people develop are not enough. The architecture is very complicated, and you can have the best strategies, but unless there are some protective factors....

There needs to be a balance of both.

Hon. Peter Kent: Exactly, and when it comes to recommendations of regulation, the Privacy Commissioner by himself would need to seek regulation, for example, in Canada, by the CRTC in terms of service providers. Have you considered that?

Mr. Owen Charters: I can't honestly say we've considered that at this point.

Hon. Peter Kent: With regard to destruction of information or the right to be forgotten, I'll ask all three of you, are you suggesting that at the age of majority there would be universal destruction of this information, or would it need to be by individual directive, ideally?

Mr. Kristjan Backman: That would not be my area of expertise, for sure. Our thought is that when the information is no longer needed, it should be destroyed regardless of how old the person is. When the purpose for which you've collected that information is no longer valid, you should have no need to keep that information and it should be disposed of properly at that point.

Hon. Peter Kent: However, as you've said, with regard to medical records, for example, we only learn of breaches of confidentiality when it's discovered.

Mr. Kristjan Backman: A well-run facility has record-keeping practices and those records are being destroyed in conjunction with those policies, so it's only in situations where somebody isn't following the policies or doesn't have a policy that you get those breaches.

Hon. Peter Kent: Then you would recommend the formation of a regulation with penalties and regular audits, or proof of—

Mr. Kristjan Backman: Our recommendation is that the Privacy Commissioner needs to have proper teeth. His office needs to have the ability to impose penalties, to make orders, and to do it proscriptively so that, in advance of a problem happening, they can go into an organization and do audits and have some powers there.

Hon. Peter Kent: Briefly, could you give an example of the COPPA penalties, from the lowest violation to the greatest?

Mr. Kristjan Backman: In our written submission we listed several of the various fines from various jurisdictions around North America, ranging from small fines all the way up to the $1.5-million range. Jurisdictions all across North America have created structures by which they impose fines for these things, based on severity.

Hon. Peter Kent: Are these fines based on individual infractions, or class or group infractions?

Mr. Kristjan Backman: I don't know the answer to that, but I could certainly find it for you.

Hon. Peter Kent: Ms. Bailey, could I get your thoughts?

Prof. Jane Bailey: We threw around the term “right to be forgotten” pretty easily just a minute ago; I did it, too. Just to be clear, to say what we mean.... What do we mean by a right to be forgotten? Even in the EU currently, without thinking about what's going to happen in 2018, it's not really a right to be forgotten. It's a right to request a delinking of your information from a search engine, which in some ways has the best of both worlds, in the sense that, practically speaking, most people are not going to go to more trouble than a Google search. If that link is no longer something that pops up in a Google search, you get effective, practical obscurity from that kind of measure, without the downside.

I am conscious of having colleagues who are interested in the Internet as an archive of our history for the future, and thinking about what full and permanent erasure might mean. Even if you said, “We'll take things off the market for 100 years”, as we do in archives sometimes, 100 years from now somebody can look at this.

I think the idea of a right to be forgotten that's a practical measure for delinking is actually an interesting practical response, provided that we have some understanding and accountability about how service providers are making these decisions when requested to make these decisions. We need accountability, transparency, and disclosure from them about how many requests they are getting, what the bases of their decision-making are, how many they agree with, how many they dismiss, and those sorts of things. I think that's a practical kind of a right to be forgotten that can give a certain amount of relief.

The other thing is, if we just did the preventative thing in the first place and said.... Just to point out, Google Classroom is used, mandated, across the Ottawa-Carleton District School Board, and we, as parents, have been assured that Google has agreed that it will not be collecting our children's information when they are using those services, and it will not be using those for commercial purposes. I guess we all believe that, because that's what they said.

To say it's not possible is more rhetoric. We have to be conscious, as consumers and citizens, that there is a certain rhetorical element to this: these things are impossible, too expensive, too difficult. We need to think about how to prevent the collection in the first place so that the destruction issues, the delinking issues, and the inaccessibility issues are not the monumental problem that they are now for a generation of kids. We can do something for the next generation of kids.

● (1610)

The Chair: We're out of time.

MP Weir, go ahead.

Mr. Erin Weir (Regina—Lewvan, NDP): Thanks very much, Mr. Chair. It's great to be here.

Great minds might think alike, because MP Kent has asked a lot of the questions that I had in my mind about the actual content of this proposed legislation. I may return to some of those points.

Something I would like to ask the panel about is their views on the mechanisms to enforce those rules, and specifically whether they have any thoughts about the proposed civil remedies.

Mr. Owen Charters: I guess I'll start.

We haven't thought about what the penalties would be. I'll be quite honest; that hasn't been our area of thought process.

We have seen this in two ways in the U.S. To ensure compliance, there have been sweeps from time to time of the sites that would be the most obvious—I am speaking especially of children and youth in these cases, sites targeted at children and youth. The other way is simply the reporting mechanism that might happen from citizens and others who are concerned about behaviours that are egregious or out of line that could be reported, so it would be a sort of self-reporting mechanism.

Aside from that, you do need something like a sweep mechanism that allows you to do what they've done in the U.S., a survey of sites and a report on compliance, with the possibility for fines and some kind of corrective measure.

Prof. Jane Bailey: I'm a lawyer. Sure, legal actions are good. I am certainly never against opening up a panoply of remedies for citizens. However, the reality of civil actions is that most people can't afford them anyway, so who would use those mechanisms? Maybe we'll be able to use them for classes and we'll get public interest organizations that can use them. We do have public interest organizations that are already trying to deal with privacy in courts. I wouldn't put a huge stock in individuals having to assert their rights. I would think ideas like audits or sweeps, where the OPC has authority to check for violations, are important.

In terms of remedies or penalties, we have to remember that we are dealing largely with market forces, so we have to make it cost more not to protect privacy and respect privacy than to just ignore it. That's what I would say about that. In effect, what this means is that the monetary penalties would have to be quite significant in many cases.

● (1615)

Mr. Erin Weir: Go ahead, if you wish.

Mr. Kristjan Backman: Sure.

In our written submission, we listed several penalties. I don't think anybody wants to see penalties be punitive for a small business that has made a mistake, but when you have instances of systematic or egregious breaches, the penalties have to be significant enough to hurt. It's sad that you have to get to that point, but unless the legislation has teeth and is backed by the Privacy Commissioner, who has the ability to enforce things, you don't move the people who are on the margins.

Good businesses are doing what they're supposed to be doing. It's the people who are on the margins who are making decisions to dispose of something or not to handle something or not to properly protect their net worth. They're making decisions on the margins because there isn't a financial penalty if they get caught doing it improperly. It's on the margins that you can move the needle. That's where people have a choice to do it right or not to do it right. You incentivize them to do it properly.

Mr. Erin Weir: One theme that underscores this act is the notion of Canadians providing consent for their information to be used in certain ways. With the proliferation of online technology, are there some practical problems with that standard? I know I'm guilty of sometimes ticking the box to agree to certain terms and conditions when I'm trying to download something or do something online. Is it realistic to make consent the standard for electronic privacy protection?

Mr. Kristjan Backman: I'm not an expert on that part of it, for sure. With regard to youth, I think you need to have more than just consent. I think you have to have protection before consent. You have to have the mechanisms to protect people before saying, “Click here to agree with our sharing your information”. You have to do it to a higher level. As adults, we have the choice to click “yes” without reading the box. Children don't....

Prof. Jane Bailey: I wouldn't limit it to young people. This isn't about infantilizing adults or saying that people are stupid. This is a group of well-educated people in this room, and I'm sure most of us have no idea what we've agreed to in the privacy policies we've agreed to and would not have the capacity to understand most of the things that are being done with our data; nor would the data service providers be able to provide us with a comprehensible explanation of it. I'm sorry, I'm like a broken record, but consent in those circumstances is a word we say to make ourselves feel better about the horse we've unleashed from the barn that is just about to run over us.

Dr. Rachel Gouin: I would also add that in some instances, you have to check that box in order to even use the application. A young person who wants to use Instagram thinks, “Of course I want to use it”, so it's a choice between using it or not. You don't have the choice to say, I want to use it, but please don't use my information. That's not one of the options.

Mr. Erin Weir: Absolutely.

Go ahead.

Mr. Owen Charters: I would just add that the problem is that young people check the box without recognition of.... I'll give you the opposite example, which is that I think, as an adult, many of us feel guilty for not having read all the terms and conditions, at least for a split second before we check the box. We know we should have. I don't think young people who have grown up using the Internet think twice about the fact that they checked that box. Checking that box gives them the access.

Yes, I'd love to have a broader debate about consent and what it means, but at the very least I think there needs to be an acknowledgement that the momentary split-second reaction that I should read those, that I should know.... There have been humorous examples of sites that have popped up saying, “You've just agreed to buy a flock of lambs”, or whatever else, and “Maybe you should pay more attention to these terms and conditions.”

At least in these cases, we need to make sure there's a second thought given to the idea of consent.

The Chair: That's time, Mr. Weir.

The next seven-minute round goes to Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon. Thank you very much for coming here today.

I want to pick up on this idea of consent. I don't want to kill the idea totally.

Some people have suggested that maybe consent should be defined differently, in the sense that there should be a model of consent to which all these service providers or the people who are using the data could agree, with a certain stipulation of agreed-upon rules whereby that model would be defined clearly for all those companies. Then, if a company or an organization were to step outside of the rules, they would highlight which rules, first to make for less reading but also to be more specific about how they were going to use that information differently.

Now, I know, Ms. Bailey, you're not a huge fan of consent. I'm just trying to see—

● (1620)

Prof. Jane Bailey: I'm a big fan of consent. I just think that in some circumstances it isn't realistic, and I'm afraid this is one of them. It's interesting to have service providers agree on a model of consent, but what that means is that they're going to have to agree on what algorithms are going to do. I actually don't think that's feasible. I'm a professor, so feasibility isn't usually a big deal with me. I usually put feasibility to the side and talk about principle, so here I am using my own argument against me.

First of all, I'm not sure that's feasible. Even if there was going to be agreement about what algorithms will do and what they won't do, most service providers don't want to disclose what their algorithm does because it's how they make their money. There's an intellectual property there that they don't want to share.

I worry that the more we build up people's idea that we shouldn't worry because we've taken care of consent, the more we'll lose sight of the fact that we're dealing with something that is so difficult to know. Maybe if we thought about regulating the processes by which information is being dealt with, then we could say we've created an environment where consent or informed consent actually makes some sense.

Mr. Raj Saini: Is there anybody else?

Mr. Kristjan Backman: I just say good luck.

Voices: Oh, oh!

Mr. Raj Saini: The second question that was raised was the question of penalties. Right now, as you know, the GDPR is going to come into effect next year and we will have to analyze our own privacy controls in regard to that. Right now, in the GDPR there are two levels of penalties. One is 10 million euros or up to 2% of annual revenues, and the second level is 20 million euros or 4% of annual revenues.

How are we going to adjust that because, obviously, there's a huge discrepancy between European companies and Canadian companies. That's what the level of the penalties are right now, and I know that we're nowhere close to that. How would we...?

Mr. Kristjan Backman: I think Canada has to make choices as to what will work for Canada. We don't have to take the United States model. I don't think that's necessary.

Mr. Raj Saini: It's the GDPR model.

Mr. Kristjan Backman: Or the GDPR model. We have different cohorts, different regulations and rules. We can set our own, but it should be meaningful and it should have enough teeth to make sure people comply with it. You can tier it, you can do all sorts of things there. It can be an absolutely “made in Canada” model for sure. I don't think we have to take the European model and say 4% and 2%. That's your job.

Mr. Raj Saini: Ms. Bailey.

Prof. Jane Bailey: I agree with that.

Mr. Owen Charters: We haven't really thought deeply about it.

Mr. Raj Saini: Okay.

Mr. Backman, one of the things you wrote is that you had an amendment for PIPEDA that would require an organization to destroy data once it was no longer needed. Can you give us an understanding of how someone or how an organization would come to the conclusion of when they felt the data was no longer needed? I think that's very subjective.

Mr. Kristjan Backman: In lots of industries it's not subjective at all. Certainly, CRA has rules with regard to how long you're keeping.... Financial institutions, the doctors, the lawyers, all have governing bodies that assist them in developing document-retention policies. There's a reasonableness test there, that when you reasonably no longer need that data, it's time to make it go away, unless the law says you have to keep it for a longer period of time.

Coming up with a policy for when documents should be destroyed is not a difficult process at all. Most companies have a retention policy as to how long they're going to keep documents. That's not the biggest hurdle there, for sure.

Mr. Raj Saini: Ms. Bailey.

Prof. Jane Bailey: It's kind of like the current provision that talks about accuracy and completeness in the principles in PIPEDA. It's because it's kind of amorphous that it becomes difficult to use it or to know when an organization is.... In some cases, no. Maybe in health care, no. Maybe in the context of health care, or those kinds of situations, you might be able to know.

Mr. Raj Saini: As a pharmacist, I know we have to keep prescriptions for two years.

Prof. Jane Bailey: Right.

In the online context and the data that's being kept by service providers, it's supposed to be accurate and relevant to the original purpose for collection. If the original purpose for collection is to use it to create aggregates for marketing, then when does it ever not become relevant? I think it is difficult to do that. I think the reason these principles are general is that to say something specific would not work for all the kinds of data you're dealing with.

● (1625)

Mr. Raj Saini: Ms. Bailey, you've written quite extensively on young people, and one of the things you've written is that they should be included as part of the conversation. When should they be informed? At what age, roughly, should they be asked to be part of the conversation?

One of the things you wrote was that "Young people have... strategies and norms to mitigate this danger". I want to get an idea of what you meant by that.

Prof. Jane Bailey: One of the first times that young people testified in a formal hearing, either in the House or in the Senate, was in the conversation around bullying and cyber-bullying. I think that is a really interesting model of bringing forward young people to engage and to testify.

I'll put in a plug for what our youth summit, the eQuality Project, is planning in 2019. We're hoping to bring young people together to talk about the Internet and what they want.

Mr. Raj Saini: Is that before October 2019, or after October 2019?

Prof. Jane Bailey: It is in 2019.

We're hoping to bring young people together to talk about the Internet and what they want, and privacy will be a big part of that. If any of you would be interested in being part of that, you can let me know.

However, that's an informal process. We should start thinking about formal processes that look a lot more like the human rights committee in the Senate, where hearings were held on bullying and cyber-bullying. These things do directly affect young people, and they often affect them in different ways than they affect adults.

The Chair: Thank you, MP Saini.

MP Gourde, you have five minutes.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

I would also like to thank the witnesses for being here.

I have concerns about big data and the fact that many organizations can collect it on all Canadians in different ways, with or without their consent.

Can Canadians request that their personal files become shadow-files again and that the big data on them be erased? Can Canadians demand that?

[*English*]

Prof. Jane Bailey: Under the current law, no. Then I guess the question is whether you are saying that erasure of their files is something that Canadians ought to be able to demand.

If you go back to the principles—and I want to use the right terms—accuracy, completeness, and being up to date, there are principles that require organizations to consider whether the material they're holding is accurate, complete, up to date, and still necessary for the purposes for which they're holding it.

They collected it. There is some case law of complaints around people saying that their file ought to have been erased and it wasn't. It was no longer accurate or complete. That may be a mild form of the sort of right you were talking about, where you're asking to have your file deleted completely.

Young people we talk to want to be able to go to Facebook, for example, when they're finished with Facebook, and say, "I'm not just closing my account, I want the record of my account deleted. I don't want you to have a backup of that on a server somewhere."

We've talked to young people who said they would very much like to have the right to do that.

[*Translation*]

Mr. Jacques Gourde: Does anyone want to add anything?

Mr. Owen Charters: I've been CEO of an online fundraising company, and I can tell you that, technically, it's entirely possible to erase a file. The engineers who handle the coding can add an option or something else to the server. It's entirely possible.

● (1630)

Mr. Jacques Gourde: Mr. Charters, since you represent an organization for youths, I will continue to ask you some questions. Today, a lot of data is collected on youth, even those under 13 years of age, because they are very active on social media.

Could the information that can be obtained through their personal profile harm them in the future?

Dr. Rachel Gouin: The answer is yes. I have a teenaged girl. I have seen the ads that show up on her Facebook profile. These are things that affect self-esteem or ads for beauty products. It is assumed that teen girls aged 13 or 14 are concerned about their weight and their appearance. It is causing them harm now and could also harm them in the future. I think it has an impact.

That's why it's important to consider the option of erasing data when young people reach the age of majority. They may have the chance to get their acts together or at least use social media by starting from scratch.

Mr. Owen Charters: It's also a question of employability. As we know, teens are forming their personalities. The same thing happens when an adult makes a decision. The young person wonders who he is, what he wants to study or what job he wants to have. I think it's very important. So the answer is yes, absolutely.

Mr. Jacques Gourde: Young people aren't generally aware of the fact that one click can have an impact on their personal image.

Mr. Owen Charters: Exactly.

Dr. Rachel Gouin: I consulted with our youth council and talked to them about this before we drafted the letter that we submitted to the committee. In fact, it seems that young people don't think about the consequences. They weren't really interested in the topic and hadn't really thought about security issues.

I think the consultations should include an education component. If we want young people to get involved and have informed opinions, they need to know what's going on. I am sure that some young people are aware of this but, generally speaking, they haven't given it much thought.

[*English*]

The Chair: We're out of time.

Thank you, MP Gourde.

MP Fortier.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, Mr. Chair.

Since today is Franco-Ontarian Day, I will continue in French to make sure that we can hear you.

First of all, I would like to thank you for your presentations, which were very interesting. Since many colleagues have already asked the questions I wanted to ask, I will instead talk about retaining and destroying personal information.

Mr. Backman, my understanding is that the industry was concerned about the costs of retaining or destroying information. Could you tell us about the actual costs and processes that can affect the industry in this regard?

[*English*]

Mr. Kristjan Backman: Sure, I can be general on that.

There are steps that good businesses take to protect the information of their customers and their employees, for example document destruction, shredding the paper documents that are in there, and dealing with their old electronic devices, their servers, their PDAs, their cellphones, things like that. These are not onerous costs for a business.

For small companies, it would be in the range of several hundred dollars a year. In large corporations it might be significantly more than that, but again, it's a very small fraction of the cost that it took to manufacture that information, and I like to look at it that way. When you look at the cost of creating the files and collecting the information, storing it and analyzing it, the actual cost of disposing of that information is a very small fraction of the amount it cost you to aggregate the information in the first place.

There's no cost to the destruction of data that is prohibitive to doing it properly. The industry is remarkably competitive across North America, so there's no issue there where a company would be making a choice other than pure bottom-line dollars to not do it correctly.

● (1635)

[*Translation*]

Mrs. Mona Fortier: Thank you.

I was concerned, for businesses, that it was a barrier to good data management, especially when it comes to retaining it or destroying it.

We have also talked a lot about Canada and some practices around the world. Should we consider other practices outside of Canada, or other measures from your analysis that we may not have had the opportunity to review?

Ms. Bailey, do you want to answer first?

[*English*]

Prof. Jane Bailey: Generally, in the area of privacy, I think of the EU as a leader and the reason for that is that they treat privacy as a human right. I think when you come at privacy as a human right, you start to see things a little differently and when you look at a market like digital communications, for example, you start to understand the costs associated with maintaining privacy are costs that are associated with respecting and honouring basic fundamental human rights.

The EU has been a leader in that regard and I think they have been courageous in the face of industry. When industry has made threats and said things were impossible, they have gone ahead and stood their ground and said we have a job to do and protecting basic human rights is one of them and here is our bottom line. It's the same as we've done with environmental issues. For instance, paper companies used to like to dump garbage into rivers. We said, you'll have to stop that and they said, that's going to cost a lot of money. We said, okay, because as a community, basic access to safe water is a fundamental part of who we are.

That's a long-winded way of saying that I do look to the EU. I think COPPA in the U.S. is a really interesting mechanism for protecting children's rights as well.

The Chair: Ms. Fortier, you have 15 seconds left.

Mrs. Mona Fortier: I slotted this time for whatever you wanted to add, but if not, that was my question. Did you want to add?

Mr. Kristjan Backman: I'll just add that in 1990 when we passed PIPEDA, Canada was the forefront of privacy legislation. We moved the needle across the globe and in a lot of ways the GDPR is the next step of our initial legislation. It's just that we went to sleep on this for 20 years, so it's time.

The Chair: Thank you.

MP Kent, you have five minutes.

Hon. Peter Kent: Thank you. I'll split my time with Mr. Gourde.

My question to all of you is this. Given the rapid pace of technological development, do you have thoughts or concerns about the cloud as opposed to device-stored or corporate-stored or hard-frame stored data and information? Can one ever absolutely be sure the information that an individual wants to be destroyed will be absolutely destroyed?

Mr. Kristjan Backman: I think we can have the policies in place to protect the consumer if their information is not destroyed properly, but I don't think you can protect people from bad actors who aren't handling the information properly. There's going to be those people out there. The question is, when you find those people, what does this legislation do and how does it prevent other bad actors from acting similarly? Can we find them? Can we rectify the situation and can we make an illustration to other people not to act that way?

Hon. Peter Kent: Do you believe content on the cloud can be policed?

Mr. Kristjan Backman: I don't think it's significantly different from content that's sitting on a server in my office or in your office or here. The information is the information, where it resides I don't think makes that much difference.

Prof. Jane Bailey: When the word “cloud” started circulating and people were getting all crazy about the cloud and worried about the cloud, someone very high up in the industry said, I just laugh when people talk about the cloud. What is the cloud? The cloud means that your data is stored on a server in some remote location. It's not actually in the ether, so giving us that sense that we can't regulate clouds.... One of the problems is that it will be a jurisdictional issue. Where physically in the world is this server situated? That is an issue.

Hon. Peter Kent: Exactly.

Prof. Jane Bailey: That's why international agreements become very important as well as trying to have countries keep pace so that nobody becomes the lowest common denominator.

● (1640)

The Chair: Jacques.

[*Translation*]

Mr. Jacques Gourde: We talked a lot about youth earlier, but I would like to talk about seniors aged 60 to over 75. These people are probably more likely to get scammed through big data or emails they receive. If people are scammed once, they end up in a database and are targeted every two weeks using the same process. It repeats itself.

Have you ever seen that kind of situation?

[*English*]

Prof. Jane Bailey: I have not done work on the elderly, so I wouldn't be any more informed than anybody else who reads about all the fraudulent mechanisms by which vulnerable elderly people have money and other important things taken away from them. I couldn't comment specifically based on research.

[*Translation*]

Mr. Jacques Gourde: Let's go back to youth. Surely you have some advice to give them. What can we advise them so that they pay attention to the future?

[*English*]

Mr. Owen Charters: It's a good question. For us, we have found that most fundamentally they need information frequently and often about good practice. That information exists, by the way. It is out there. I think there needs to be more resources put behind ensuring.... There was a conversation about putting it in a curriculum. There are conversations about making sure it's more widely available, and persistent, in that sense. There have been campaigns about personal information protection in general. I think we need to do a lot more to ensure that young people are cognizant of the risks they're taking on an ongoing basis.

Prof. Jane Bailey: I would just add that I think education is important, too, but one of the ways I'd like to see education changed in this regard is not only to educate kids how to protect themselves, but to educate kids on what their rights are and on the practices that the media industry is engaging in that infringe on those rights, and what they can do about that. How can you advocate for your rights?

I feel that's a piece that's missing because we're so concerned about protecting children, as we should be, and we forget. When we teach kids about crossing the road, we also have laws that put people in jail for running stop signs. A lot in the Internet context has been focused on telling kids how to behave instead of saying, “Let's scan the environment to see what we're doing or what we could be doing that would make it a heck of a lot easier to exist in these spaces in a way that's healthy now and in the long term.”

The Chair: MP Dubourg.

[*Translation*]

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

I would like to welcome the witnesses here today and thank them for their presentations.

Ms. Bailey, my first question is for you.

I know you are looking more specifically at the youth approach, but the system is complex. We talked about the right, from the age of 18, to erase all of their personal information and start over from scratch. What do you think of the fact that companies have information on young people under the age of 18? Should parents be given the right to erase this data at all times?

[*English*]

Prof. Jane Bailey: The other issue is that, when you talk to young people about privacy, one of the groups of people they need privacy from are their parents. This is a healthy part of growing up. They need privacy from their parents, in particular at ages when they're exploring issues around identity, whether it be gender, sexual identity, or sexuality. It's very important for them to be able to have privacy from parents on these issues.

An overarching parental right that says the parent should be the person who has the absolutely authority to makes these decisions, I have some hesitations about.

● (1645)

[*Translation*]

Mr. Emmanuel Dubourg: It is true that it has become very complex. There was a time when we could block certain things on our televisions, but now young people are so skilled that we can't get around them.

Mr. Charters, you said young people needed to be informed. I don't know if you are aware of the approach that is being taken in Quebec in this regard. People from the Quebec government go to high schools to educate young people. Should such practices be extended or suggested in other situations?

[*English*]

Mr. Owen Charters: I don't know that I'm aware of the specific curriculum piece in Quebec, but we're seeing that every jurisdiction, especially in its curriculum, has come up with different approaches to this. That's part of why we've advocated for some federal leadership, because we're finding that there is real unevenness in this and we don't think it's a curriculum issue. It's not the same as math, reading, writing. Those are curriculum issues. These are about privacy, and I think they're about rights.

To Ms. Bailey's point, I think that's the fundamental piece. If we're talking about rights, then this has to happen not just in one province, although that definitely shows leadership, but needs to be something that's more consistently approached. But it may be good practice.

[*Translation*]

Mr. Emmanuel Dubourg: All three of you agree to give more powers to the commissioner and even to go so far as imposing penalties.

Mr. Backman, given the nature of your organization, you say that this should be done, despite the fact that your clientele would be subject to those penalties.

Should penalties necessarily be monetary or could they take other forms, such as taking away the licence? Should there be a range of penalties?

[*English*]

Mr. Kristjan Backman: I think that money is probably the easiest one. It's the easiest one to target. We've had “name and shame” for years, where the Privacy Commissioner can name you and publish your information. There is certainly some reputational risk there. There have been some teeth, but you have to find something you can do, and money is certainly the thing that everybody has a little of. If you're going after something, that's the easiest. I think it should be up to you guys to craft rules on where you want to go.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

[*English*]

The Chair: We'll have a three-minute round with Mr. Weir, and then that's it. If anyone has any further questions, we'll put you on the list.

Mr. Weir.

Mr. Erin Weir: Thank you.

I normally sit on the government operations committee and we look at the appointment process. Given the role that the Privacy Commissioner would play in applying this legislation, I'm wondering if you have any thoughts on what qualifications or criteria we should be looking at when appointing privacy commissioners.

Prof. Jane Bailey: I'll go back to what I said about the EU. I think we should be interested in a Privacy Commissioner who understands privacy from the perspective of human rights. In the process of writing a paper, I was just reminded that privacy didn't make its way explicitly into the charter. Part of the conciliation for that was the creation of the Office of the Privacy Commissioner of Canada.

Someone vested with the responsibility of administering quasi-constitutional rights has to be somebody who views privacy in the context of constitutional rights from a human rights perspective and prioritizes that perspective in decision-making.

● (1650)

Mr. Erin Weir: We've talked a little about removing the personal information of younger people. I'm wondering if panellists think there should be an upfront prohibition on the collection of personal information of Canadians below a certain age.

Mr. Owen Charters: We didn't argue for a prohibition, but I think it's like other questions of privacy—it has to be about what's appropriate and needed for the transaction. Since transactions tend to be pretty notional at the age of minority, this should be pretty limited. I wouldn't call it a prohibition, but it means you're not collecting very much. I think there has to be a greater understanding of what that actually means. You don't need to provide a lot of information at a young age to access a site that allows you to take your character through the maze, for example, or learn math. I think we have to consider what it's being used for.

Mr. Erin Weir: I would also invite comments on the desirability and feasibility of requiring social media companies and other online providers to disclose their algorithms.

Prof. Jane Bailey: I think it will be a problem because they have become the fundamental basis for making money in a "data in exchange for services" market, which is what the Internet has become. Just asking them to disclose the programming of their algorithms is likely to yield some fairly significant resistance in the market. This may be one reason why it makes it easier to say there are certain things you can't do, there are certain people you can't collect information from, or there are certain things you can't do with that data once you collect it. It avoids the problem of trying to compel disclosure of something that I think would be met with resistance.

Then there's the fact that you'll have algorithms that nobody can explain to you in human terms. You can say to disclose it, but then someone will come here and.... If they can understand it, you won't be able to, and sometimes they won't be able to understand it themselves. With machine learning, that's the point. The machine is teaching itself.

The Chair: Thank you, MP Weir.

We have two others. We have five minutes left, so there are about two and a half minutes each.

MP Erskine-Smith and MP Baylis.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): First, for the Boys and Girls Clubs, you mentioned parental consent, verifiable consent. I'm not exactly sure what that means. If I were to play online poker in the U.K., for example, would they require that I send my driver's licence and see a piece of ID? What are we talking about when we talk about verifiable consent?

Mr. Owen Charters: It depends on the sites. There have been ways where there's a verified account provided by a parent, which then verifies the underage person's account. It could be ID or it could be something simpler, depending on the risk.

Mr. Nathaniel Erskine-Smith: Such as a Facebook account or something...?

Mr. Owen Charters: Absolutely.

Mr. Nathaniel Erskine-Smith: Okay, you did note that you liked Ms. Bailey's mention of perhaps moving beyond consent.

When we look at models around the world, is there a gold standard we should be looking at, Ms. Bailey, in terms of moving beyond consent?

Prof. Jane Bailey: I don't think there is. Again, I go back to the way the EU approaches it. The more you create rights to not have your data used in particular ways or collected for particular things, the more you foreclose industry's being able to dictate that in their terms of service, creating this illusion of consent by having people click "I agree to the terms of service".

Mr. Nathaniel Erskine-Smith: I think the EU still allows the use of data for reasonable business practices.

Prof. Jane Bailey: Yes, I agree, so when you said there's a gold standard, I said there wasn't. There isn't.

Mr. Nathaniel Erskine-Smith: Okay.

Prof. Jane Bailey: In the ultimate model that I'm thinking of, I don't think there's anybody who's doing that.

Mr. Nathaniel Erskine-Smith: It strikes me, when you mention discriminatory practices, that it's a very compelling example. Obviously discriminatory practices, regardless of age, should be outlawed—full stop. But the use of data itself for reasonable business practices doesn't strike me as a particular problem. I recognize that I may not understand the algorithm behind it, but I do understand what it means to use my preferences to advertise to me based on those preferences.

I worry that when we talk about not understanding the algorithm, then we undo the ability of businesses to advertise or to use the data in a meaningful way that a lot of consumers would appreciate.

● (1655)

Prof. Jane Bailey: Yes, except that businesses can't now make decisions that violate human rights codes. If they come up with mechanistic ways of doing that and it makes it impossible for us to know whether that's happening or not, they're still violating human rights codes. That was my point.

My point is that part of machine-based decision-making is that we don't get to see that, so we may miss discriminatory practices that we might otherwise pick up in human-based decision-making. One way of addressing that is the example from the GDPR that says, for certain kinds of decisions, you have to be able to provide an explanation. That will mean that you'll have to be able to provide an explanation that is humanly understandable.

The Chair: Thank you, MP Erskine-Smith.

MP Baylis, you have the last two and a half minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): I just want to follow up on those questions that Nate was asking, and I understand there's no perfect solution.

What are the best practices? I've heard of jurisdictions such as the U.S.A., California, the EU, and the right to erase, the right to be forgotten, some general data protection under 16, under 13. What would it be if you had only one that you could implement? Which one would you choose?

We'll start with you, Mr. Charters.

Mr. Owen Charters: We actually put it in our recommendations. We didn't pick a jurisdiction, but we said that we want the capacity for parental consent to be a requirement under the age of at least 13, with the right to be forgotten by the time you reach the age of majority. The combination of those two is sufficient at this point in time.

Mr. Frank Baylis: Does that exist anywhere?

Mr. Owen Charters: It's a combination of the United States' COPPA and the European model.

Mr. Frank Baylis: Combine those two, okay.

Mr. Kristjan Backman: I would go at it a little differently, and the GDPR is pretty good on this. It's the privacy by design. You say, from the very first steps when we're collecting information, that we are designing the system around protecting that information. We think of the protection of that information first, before we start to think about how we're going to analyze it, how we're going to deal with it, how we're going to sell it, how we're going to market it, and that becomes a requirement of each individual organization as they're building their data collection.

Mr. Frank Baylis: Who has that kind of a law in place?

Mr. Kristjan Backman: The GDPR that is coming in. “Privacy first” or “privacy by design” is what they call it.

Mr. Frank Baylis: It's not in place yet, but it's coming. Is that correct?

Mr. Kristjan Backman: It's coming this year.

Prof. Jane Bailey: With respect to young people, I would say that we should prohibit companies from collecting and using their data for profiling and marketing purposes. That's a beginning. That doesn't address all the other things I talked about.

Mr. Frank Baylis: Does someone do that right now in any jurisdiction?

Prof. Jane Bailey: No.

The Chair: Thank you, MP Baylis.

Thank you, guests, for coming today. It was a very thorough conversation with a limited amount of time.

Just for the committee's understanding, they were invited before but it was pre-empted by some parliamentary business.

We're going to suspend, folks, for about five minutes until our guests can exit. Then we'll get into our committee business.

[*Proceedings continue in camera*]