HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 060 • 1st SESSION • 42nd PARLIAMENT

**EVIDENCE**

## Thursday, May 11, 2017

---

## Vice-Chair

**Mr. Nathaniel Erskine-Smith**

# Standing Committee on Access to Information, Privacy and Ethics

**Thursday, May 11, 2017**

● (1530)

[*English*]

**The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)):** Welcome, everyone, to meeting number 60. We will pursue and continue our study of PIPEDA.

Today we're joined by the Canadian Wireless Telecommunications Association, with Robert Ghiz. We have Linda Routledge and Charles Docherty—from East York particularly, my riding—from the Canadian Bankers Association. We have also Wally Hill and David Elder from the Canadian Marketing Association.

Welcome, all.

We'll start with Robert Ghiz for 10 minutes. Everyone will have an opportunity to present for 10 minutes, and we'll proceed with questions from there.

**Mr. Robert Ghiz (President and Chief Executive Officer, Canadian Wireless Telecommunications Association):** Thank you very much, Mr. Chair and committee members, for this opportunity to provide the perspective of the Canadian Wireless Telecommunications Association, to which I will refer as the CWTA, on the Personal Information Protection and Electronic Documents Act.

This is new to me, so bear with me. I sat on these committees for 12 years, but I was in your seats. Now this is a bit of a different perspective for me. I'll do my best.

CWTA represents member companies from every part of the wireless sector, including wireless carriers, equipment manufacturers, and other businesses that provide services and products to the industry. Over the past 30 years, Canada's wireless carriers have made more than $42 billion in capital investments in wireless infrastructure, and they continue to invest at the rate of more than $2.5 billion per year. These investments are paying off. Today, 99.3% of Canadians have access to Canada's world-class networks.

[*Translation*]

With 5G technology at our door, the entire wireless communications sector is working to maintain its role as a driver of innovation.

Maintaining the flexibility of the Personal Information Protection and Electronic Documents Act and applying it fairly to all sectors will also help foster innovation.

In his testimony, the Privacy Commissioner highlighted the main strengths of the act: it is technologically neutral, and it is based on general application principles.

The commissioner suggested four issues to guide your study: consent, reputation, enforcement powers, and the adequacy of the Canadian regime compared with the new European regulation.

My comments will focus on the impact of those four issues on the ability of the wireless sector to serve its clients, as well as on its ability to compete and innovate in the digital economy.

● (1540)

[*English*]

On the issue of consent, the commissioner suggested that relying on consent alone may no longer be reasonable in every possible circumstance, given the impact of technology. To that I would first paraphrase a comment submitted by one of our members at the Privacy Commissioner's consultations on consent, that as technology evolves, so do customers' appreciation and understanding of it.

The care that our member companies take in being transparent with their customers about how they are processing personal information—for instance, through clearer privacy policies—is a key part of their trust relationship with their customers. The most important asset for doing business in the 21st century is trustworthiness, and our members are well aware of it.

As for the application of the consent principle, the fair and equitable application of this across industry sectors is essential to our members' ability to compete in the digital marketplace and to preserving consumer trust in the digital economy. What we refer to as the wireless sector is roughly 30 years old, which is younger than a good portion of the companies we represent, yet today Canada's dynamic wireless sector is responsible for close to 139,000 full-time jobs and $13.3 billion in direct GDP contribution. To continue to grow, innovate, and compete with larger global entities, our members must be confident that the rules will apply the same way to Canadian companies as they do to non-Canadian players. This symmetry in the application of the rules also benefits consumers, who would be right to expect their personal information to be treated similarly in similar contexts.

We would suggest that expanding the definition of what is acceptable use for legitimate business interests could provide more clarity in that regard. For instance, in the European Union, personal information can be used for purposes that support the data controller's legitimate interests so long as these purposes are not incompatible with the original purpose for which the information was collected and so long as it does not violate the fundamental rights and freedoms of the data subject. Such a model would allow our members to innovate and compete on the global stage in a way that respects people's fundamental rights and the business relationship that already exists between companies and their customers.

On the issue of reputation, several witnesses have suggested that Canada may want to follow Europe's lead and include an explicit right to be forgotten into its legislative framework. In practical terms, the European right to be forgotten requires that commercial entities receive complaints directly from individuals, that they evaluate the merit of these complaints, and that they alter their systems as required. I am not one to advise the committee on whether a European-style right to be forgotten strikes the right balance between privacy and freedom of expression for Canadians. However, I do urge the committee to be mindful of the potential burden such measures could place on the operations of Canadian businesses involved in the digital economy.

On the issue of enforcement powers, the Privacy Commissioner suggested that stronger enforcement powers would foster greater compliance with PIPEDA. CWTA believes the current ombudsman model is best suited to the current principles-based framework. A collaborative relationship between industry and the regulator is more efficient, and results in better outcomes for consumers. By investing the commissioner with the power to issue fines and impose orders, Canadian businesses would find themselves in an adversarial relationship that would discourage the informal and expedient resolution of complaints, which would be to the detriment of consumers.

As it stands, the commissioner is already naming companies that are deemed to be in violation of PIPEDA. The potential reputational damage from a finding of non-compliance by the commissioner is a sufficient deterrent, given the importance of consumer trust in the digital economy. We would argue that fines would be no stronger a deterrent than the damage to business reputation.

In the specific case of breaches, we are anticipating the coming into force of mandatory reporting and record-keeping requirements, which were added to PIPEDA through the passage of the Digital Privacy Act in 2015. These provisions will be supported by fines of up to $100,000. Breaches themselves are already subject to class action. We submit that the principles-based structure of PIPEDA does not call for enforcement powers. It would be better served by regular guidance from the Privacy Commissioner. Proactive guidance from the commissioner could explain how PIPEDA's general principles should be applied to new business models. It is ultimately not fair to consumers that the companies they do business with should have to wait for complaints to arise in order to develop policies on personal information management for new business lines.

One specific example is the Privacy Commissioner's upcoming guidance on connected cars. The connected car—and in a few years from now, the automated car—is one example of the many social benefits that will come from 5G wireless networks. As such, CWTA shares the Privacy Commissioner's concern with getting privacy right early on in the process. We hope to have the opportunity to share our industry's perspective on this with the commissioner and future guidance documents.

On the issue of preserving Canada's adequacy status with the European Union, I will say that our members recognize the importance of maintaining Canadian businesses' ability to operate on other continents, just as foreign Internet companies compete with us on our own turf. We would urge the committee to take into account the operational repercussions for Canadian companies of any legislative changes made to the Canadian regime.

[*Translation*]

In closing, I would once again say that we are determined to maintain our strong record in terms of complying with the act and our good relationship with the commissioner. The current model supports a collaborative approach with the commissioner. That has enabled us to emphasize positive results for our clients.

[*English*]

Thank you very much for your time today. I will be looking forward to questions after.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much, Mr. Ghiz.

Next, representing the Canadian Bankers Association, we will hear from Linda Routledge and Charles Docherty.

**Ms. Linda Routledge (Director, Consumer Affairs, Canadian Bankers Association):** Thank you very much, Mr. Chair, and good afternoon.

My name is Linda Routledge, and I'm the director of consumer affairs with the Canadian Bankers Association. With me today is Charles Docherty, our senior counsel. We are pleased to be here today to discuss the Personal Information Protection and Electronic Documents Act.

The CBA works on behalf of 62 domestic banks, foreign bank subsidiaries, and foreign bank branches operating in Canada and their 280,000 employees. The privacy and protection of clients' personal information is and always has been a cornerstone of banking. Given the nature of the services that banks provide to millions of Canadians, banks are trusted custodians of significant amounts of personal information. Banks take very seriously their responsibility to protect customers' information. They are committed to meeting not only the requirements of privacy laws but also the expectations of their customers. A former assistant privacy commissioner once acknowledged that privacy is in the banks' DNA.

The banks were among the first group of organizations subject to PIPEDA in 2001. We believe that PIPEDA has worked well to date to balance the protection of individuals' personal information with the legitimate use of personal information by organizations. PIPEDA is principles-based and technologically neutral, providing the necessary framework for innovation as well as new technologies and business models. It's generally well positioned to continue that mandate going forward. The banks would, however, like to suggest a few changes that we believe might enhance and clarify PIPEDA to make it more effective. These suggestions are related to three broad subject areas—meaningful consent, financial crimes, and access rights.

On meaningful consent, banks collect the personal information that is necessary to provide clients with the products and services they want. This information is collected according to the requirements of PIPEDA, and banks take steps to ensure that their clients understand the nature of the consent being provided. All banks have privacy policies in place and privacy officers who oversee compliance with these policies. Banks have a strong incentive to enhance their customers' ability to provide meaningful consent, because building their customers' trust is and always has been a top priority.

The committee heard from several other witnesses who questioned whether the consent that individuals provide is meaningful, given the complexity of terms and conditions when signing up for any product or service. We suggest that one way to address this concern may be to streamline privacy notices so that consent is not required for uses that the individual would expect and consider reasonable. In particular, we support the concept that express consent should not be required for legitimate business purposes. Some examples of such purposes might include the purposes for which personal information was collected, fulfilling a service, understanding or delivering products or services to customers to meet their needs, and customer service training.

Removing the requirement for express consent for legitimate business purposes would simplify privacy notices, thereby facilitating a more informed consent process where consumers can focus on the information that is most important to them and on which they can take action.

Second, the banking industry suggests that the current narrow definition of publicly available information is out of date. The current regulations reference the dominant technologies of the early 2000s, when the regulations were promulgated. We suggest that the committee should look at updating the definition with a view to modernizing it.

With regard to financial crimes, protecting the security and safety of its employees, customers, and the Canadian financial system is a priority for Canada's banks. Banks are constantly upgrading their security systems and work hard to prevent billions of dollars of financial crime each year. Banks work closely with law enforcement agencies and authorities across the country to help them with their investigations and the prosecution of suspected criminals.

● (1545)

Currently provisions in PIPEDA allow the sharing of information between organizations only where it is reasonable for the purposes of detecting, suppressing, or preventing fraud. This does not include other types of criminal activity such as theft of data or personal information, money laundering, terrorist financing, cybercrime, and even bank robbing.

To enhance the banking industry's ability to prevent this broader criminal activity, we recommend that the provisions in PIPEDA relating to disclosures without consent should use the term “financial crime” instead of “fraud” to capture the broader range of criminal activities that Canada's financial institutions deal with on a daily basis.

Further, we suggest that financial crime be defined to include first, fraud; second, criminal activity and any predicate offence related to money laundering and the financing of terrorism; third, other criminal offences committed against financial institutions, their customers, and their employees; and fourth, contravention of laws of foreign jurisdictions including those relating to money laundering and terrorist financing.

Financial crime negatively affects banks, consumers, and the economic integrity of the financial system. Banks understand the important role they have to play and have highly sophisticated security systems and teams of experts in place to protect Canadians from financial crime. We believe this amendment to PIPEDA would give banks greater ability to perform their role in this important endeavour.

Finally, on access rights, there are times when organizations create documents containing personal information related to anticipated litigation. Consistent with guidance issued by the Privacy Commissioner and provisions in the privacy laws of both Alberta and Quebec, this information should not have to be provided in response to an access request. We would ask that PIPEDA be amended to provide a specific exemption for these types of documents based on litigation privilege.

In conclusion, PIPEDA has served Canadians well over the last 17 years, encouraging organizations to protect the personal information they have about individuals and also encouraging individuals to be more aware of their rights and responsibilities to protect their own personal information. Nevertheless, as with any legislation operating in an environment that is continually evolving, there are some areas where slight adjustments and improvements would be desirable.

We hope that our commentary assists the committee with its review of the act.

We look forward to your questions.

Thank you very much.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much for your presentation.

Finally, on behalf of the Canadian Marketing Association, we have Wally Hill and David Elder.

**Mr. Wally Hill (Vice-President, Government and Consumer Affairs, Canadian Marketing Association):** Thank you, Mr. Chair.

Thank you to the committee for the invitation to appear before you today to present CMA's views on your study of the Personal Information Protection and Electronic Documents Act, also well known as PIPEDA.

CMA is the largest marketing association in Canada. It represents communications and marketing agencies as well as major brands in retail, financial services, technology, and other sectors. Our advocacy efforts aim to promote an environment in which ethical marketing prevails in both communicating with and serving customers.

CMA has provided a written submission to the committee in advance, but today I would like to focus my remarks on three issues —namely, is PIPEDA in need of amendments, does the consent model still work, and is OPC enforcement effective?

First, on amending PIPEDA, some argue that PIPEDA is broken or inadequate and needs to be fixed. However, our view is that PIPEDA has in fact withstood the test of time in addressing the new challenges of our fast-changing digital world. By deliberate design, PIPEDA was structured on core principles rather than prescriptive rules precisely in order to create a law that would be able to adapt to new technologies, practices, and expectations. The PIPEDA model promotes a more collaborative approach in developing guidance to organizations operating in a very wide range of different contexts. The OPC is in a position to provide further interpretive guidelines as social, technological, and business developments require. This framework has served and continues to serve Canadians very well.

It's also important to recognize that the recent amendments to the law, introduced in 2015 by the Digital Privacy Act, provide additional protections for individuals. These include an increased responsibility for organizations to obtain valid consent, especially for children and other vulnerable parties; mandatory breach notification requirements; and new powers for the Privacy Commissioner to enter compliance agreements with organizations and coordinate enforcement with international counterparts.

While some may argue that further amendments to the law are necessary, CMA strongly cautions against this approach. Our recommendation is to allow the amendments passed in 2015 to take full effect and then assess the impact and effectiveness of those changes before contemplating further changes to the law. For example, the new breach notification provisions that were enacted nearly two years ago have yet to come into force. We are still waiting for the publication of the related regulations that will allow those to take effect. Once the regulations are finalized, organizations will then need to train their personnel, update their processes, and basically get ready for that set of changes to PIPEDA and meet the new requirements.

The second issue I want to address is consent. CMA believes that the right mix of individual choice and a robust accountability framework will strengthen privacy and consent. With business models becoming increasingly focused on innovation, and greater customization of products and services, which is all in response to consumer expectations, the strains on a consent-based regime must be recognized. Privacy policies that are rarely read, smaller screens, and other device restrictions are realities that pose challenges to obtaining meaningful consent.

While consumer consent must still be regarded as an important element in privacy law, shifting more to a risk assessment-based model, where organizations are given more freedom but also more responsibilities over consumer data, would modernize the Canadian privacy framework to the benefit of businesses and consumers alike. In such a model, the types of notices provided and consent obtained are linked with the sensitivity or risk of harm of a given data-handling activity. This is what we see in the breach provisions that were passed several years ago. This is consistent also with schedule 1 of PIPEDA.

CMA believes that strengthening the accountability framework through self-regulatory codes of practice and other creative tools, such as data anonymization, offers the best approach to enhancing privacy protections for individuals. An excellent example of a self-regulatory initiative is the AdChoices program for interest-based advertising, developed by the Digital Advertising Alliance of Canada, the DAAC.

● (1550)

CMA is among the founding marketing and advertising organizations that launched the DAAC in 2013 in order to give consumers real-time notice and choice over whether their browsing data would be used for interest-based advertising. An enhanced accountability model necessarily comes with more responsibilities for organizations. For example, CMA's code of ethics and standards of practice imposes strict limitations on the collection and use of personal information of children under the age of 13.

My third and last point relates to the Privacy Commissioner's enforcement powers. We do not agree that the commissioner requires additional powers. In fact, the commissioner currently has the power to issue findings, audit organizations, make recommendations, and now enter into compliance agreements. The brand reputation damage, as has been noted already, that can result from an adverse commissioner finding can be significant. The impact of such negative publicity is an enforcement tool that cannot be overstated. In addition, if voluntary co-operation is not forthcoming, the commissioner has the power to summon witnesses, administer oaths, compel the production of evidence, and take matters to the Federal Court to rectify situations that remain unresolved.

CMA believes that the ombudsman model under which PIPEDA operates has been highly effective and has resulted in a high level of voluntary compliance from Canadian businesses. Consider the number of PIPEDA-related complaints brought forth to the OPC. Between January 1, 2015, and March 31, 2016, the OPC received 351 complaints. Only 52 of those cases, or just under 15%, were considered well founded by the commissioner. Of those 52 cases, 46, or upwards of 90%, were either completely or conditionally resolved.

The current ombudsman model of oversight permits the OPC to protect and promote privacy rights of individuals through positive and proactive engagement with industry associations and organizations seeking guidance on compliance and emerging privacy issues. Providing the OPC with more direct enforcement powers would undermine that open and co-operative relationship that has developed between the OPC and Canadian industry.

In conclusion, we would point to the OPC's extensive casework and published findings over the past 17 years and the great many improved privacy practices adopted by businesses over the years as a result. This is valuable evidence that PIPEDA works well in its current form.

We would also caution against positioning PIPEDA as a default, catch-all solution for issues arising from the rapid evolution of technology and data uses. In many instances, there are other laws and regulations that may be better suited to address specific sectoral concerns or other issues that arise. PIPEDA must be effective in protecting Canadians' privacy rights while also encouraging organizations to innovate new products and services for their consumers and customers. This often involves the responsible use of data, including personal information. CMA believes that the existing PIPEDA framework has demonstrated the right measures of flexibility and effectiveness in achieving these goals.

Thank you, Mr. Chairman. We welcome the committee's questions.

● (1555)

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thank you very much for your presentations, all.

We will start with Mr. Long in our seven-minute round.

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

Thank you to our presenters this afternoon. That was again very interesting testimony. The more we hear, the more we learn, and I think the more questions we have.

I'll recount my first experience with the right to be forgotten. I apologize in advance to my colleagues for maybe repeating this story, but we've had so much turnover on this committee that I guess some will be hearing it for the first time. My first test of the right to be forgotten was when I was with the Saint John Sea Dogs.

They won the President Cup title last night in the Quebec Major Junior Hockey League.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Congratulations.

**Mr. Wayne Long:** Thank you very much. That was a shameless plug there.

I remember when I was quoted in some stuff online about bedbugs. We had a teddy bear drive, a teddy bear toss, and there was a bedbug scare in our city at that point. I made the decision that we would not hand out those teddy bears to the hospitals, nursing homes, and what have you around town. Very quickly the story turned around that I was this bad guy who was denying hospitals and nursing homes these teddy bears. For years, literally years, any time you Googled “Wayne Long”, you would have this list of articles and comments about me and teddy bears. It took two years of my political career development to at least bump them down a bit.

Again, those were great presentations, but Mr. Ghiz, can we forget about the right to be forgotten?

**Mr. Robert Ghiz:** That's a very good story, which I would say pretty much everybody around this table can relate to. I can for sure.

It's the burden associated with implementing the right to be forgotten with which we have an issue. There are costs associated with it, how you track it down, and who you go through. I just think it's too much work for us to adapt to that European model. That's our opinion. It's not something that's easy to do. There is also freedom of speech; that does exist.

From the wireless association's perspective, we're not for it.

**Mr. Wayne Long:** Thank you for that.

You said that for your organization's members to grow, your companies need to be ready, and obviously I don't think it's any secret that the European GDPR is coming into effect, I believe, on May 25, 2018. Do you feel that our Canadian companies are ready for what's going to come at them?

**Mr. Robert Ghiz:** I believe our Canadian companies, in terms of wireless telecommunications, are extremely well prepared for competition. We are competitive within the Canadian market. We are an innovator in terms of our capabilities here. We're a world leader in terms of our technologies. What we're asking for in a competitive model is to make sure that any rules that exist here are equitably delivered to anybody else who wants to do business here.

● (1600)

**Mr. Wayne Long:** Should we be proactive as opposed to reactive? Should we take measurements to ensure the adequacy?

**Mr. Robert Ghiz:** Yes. We always need to make sure we're being competitive, but I think when it comes down to what's happening in Europe versus what's happening in Canada, we need to worry about what's best for our Canadian economy, and to make sure that our companies are able to compete on a level playing field.

**Mr. Wayne Long:** Okay.

Also in your presentation you talked about 5G, and you said that 5G is coming.

I see a very quick side story to that. I was with a friend in a car and he was talking about 5G and how quickly it is coming, and he said that there will be, for lack of better words, “drivable” cars sooner than we think.

I just want to get your comments on PIPEDA and whether it is technology-neutral. What changes do you see coming in the next few years?

**Mr. Robert Ghiz:** In terms of where we're at with 5G, it depends who you talk to. Some people think we're already on the cusp of 5G, but when will 5G come fully into effect, with the Internet of things and where we're operating in a sort of new world? I don't think we're going to see autonomous cars tomorrow or in a few years, but I think —

**Mr. Wayne Long:** This gentleman I was with, who obviously I won't name but who is quite involved, feels it will be within 10 years.

**Mr. Robert Ghiz:** That could be the case. I would say that with autonomous cars—and I've had the opportunity to view and visit the QNX labs here in Ottawa—there is what I would call a constant evolution. Today you have your speaker phone; when you're backing up, you have cameras; and when you're driving down the highway now and you veer a little bit offside, your car shakes for you, so it's constantly getting to that level.

In terms of its relation to privacy and PIPEDA, that's where we believe it's important for the commissioner to consult with us. Do I have the answers right now? No. My members are better at that. That's why we're asking that when the commissioner does go out to do his consultations on where we are with 5G, our members and CWTA be involved.

**Mr. Wayne Long:** Okay, thanks for the answers.

Mr. Hill, I'd like to ask you some questions. I often ask the question about meaningful consent when it comes to children.

My own opinion is that there is not enough there to protect our children, and I can certainly attest to.... My children are a little bit older, but I have friends who have younger children who are on the computer, and there is a scary amount of “clickbait” that comes up at times, and it is not controlled. I think the stats show—and I apologize for not having the exact stats—that 70% of 12-year-olds have a cellphone now.

What more can we do to protect children?

**Mr. Wally Hill:** This is a challenging area in terms of actual implementation.

I mentioned in my remarks that we have in our code of ethics stringent guidelines regarding the collection of children's data. Marketers who are doing so are required to obtain express consent from parents or guardians, but—

**Mr. Wayne Long:** If you don't mind, I just want to jump in. I apologize.

What age brackets...? I've done some reading about how there should be parental consent from—and I apologize for not having the exact numbers in front of me—

**Mr. Raj Saini (Kitchener Centre, Lib.):** It's 13 to 15.

**Mr. Wayne Long:** It's 13 to 15, and 15 and so on.

**Mr. Wally Hill:** We have some gradients. There are some issues around teenagers. Teenagers in our society start to assume a greater level of responsibility for their own activities, so our code of ethics does have different provisions for teenagers, but also more stringent provisions on the collection of data from teenagers as opposed to adults, people who have gained age of majority.

Under our requirements, children under the age of 13 are not able to give consent for the collection and use of their personal information, and parental consent should be sought.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Unfortunately, we'll have to wrap up. We're a little over the seven-minute mark. Hopefully your answer can be picked up in relation to other questions.

Mr. Kelly, go ahead for seven minutes.

● (1605)

**Mr. Pat Kelly (Calgary Rocky Ridge, CPC):** Thank you.

I would like to start with Ms. Routledge.

You said a few things in your remarks that interested me quite a bit. You spoke on behalf of the banking industry and about the narrow definition of publicly available information being out of date. I would like you to expand on that, because I'm not quite sure I understand what you mean and what the implications of that definition are.

**Ms. Linda Routledge:** When the publicly available information regulations were promulgated, they talked about telephone books, professional directories, and so on, with that type of information being considered publicly available. Now people voluntarily put their information online and in any other media. Technology is opening that up more and more.

We feel it would be advisable to think about looking at those regulations and maybe modernizing them so that they're not just restricted to these databases that were in existence in 2001.

**Mr. Pat Kelly:** At present, is there is a tight definition of what constitutes publicly available information?

**Ms. Linda Routledge:** The regulations set out, I think, five or six categories for the exact type of information that can be considered publicly available.

**Mr. Pat Kelly:** Would you favour a broader definition or a narrower definition?

**Ms. Linda Routledge:** I would favour a broader definition that would be more technologically neutral.

**Mr. Pat Kelly:** Okay.

You devoted a full section of your remarks to financial crimes. You spoke about “financial crime” and using that language rather than references to fraud.

I have a background in the mortgage business. I was in it for many years and am aware of many different scenarios and have taken a lot of training on the prevention of fraud. In fact, I even taught those coming into my industry about fraud prevention.

How do you see PIPEDA? What is the intersection or interaction between PIPEDA and fraud prevention?

**Ms. Linda Routledge:** In PIPEDA there are exceptions regarding disclosure without consent, under which banks can disclose to other organizations only in instances of fraud.

**Mr. Pat Kelly:** Does PIPEDA prevent you from co-operating with other entities?

**Ms. Linda Routledge:** It does certainly restrict us, because it's restricting it to fraud. There are other things like bank robberies, money laundering, and so on, that certainly aren't fraud but they are definitely criminal activities. We would like to have the definition broadened or the concept broadened so that for the rest of these types of crimes, the banks can share information with other organizations and other banks.

**Mr. Pat Kelly:** Is there appetite among your members for sharing for that purpose?

**Ms. Linda Routledge:** Actually, before PIPEDA was amended, we had the bank crime prevention and investigation body. It facilitated the exchange of this type of information among the banks, but with the most recent change to PIPEDA, we've taken away investigative bodies and now we have these two exemptions from disclosure. The problem was that instead of saying “criminal activity”, the exemption said “fraud”. That definition limits what the banks are able to do.

**Mr. Pat Kelly:** I would have thought it would be the other way around—that fraud, being either civil or criminal, would set a lower bar for what you would be allowed to share.

**Ms. Linda Routledge:** I can ask my legal counsel to opine on that one, if you'd like.

**Mr. Charles Docherty (Senior Legal Counsel, Canadian Bankers Association):** Our view would be that the definition of fraud as used there is limiting, in that we are dealing with crimes. In that circumstance, it's to prevent, suppress, and detect fraud, so our interpretation is that it's fraud as defined in the Criminal Code of Canada, which is why we are looking for an expansion to include financial crime.

Really, what the banks are focused on—and other organizations that are able to use this exception—is to combat crime. That's what our focus is.

● (1610)

**Mr. Pat Kelly:** I find it quite refreshing and I am quite pleased that your organization is talking about the desirability of sharing information for the purpose of combatting financial crime. There is a perception in the industy that your membership is not keen on sharing information and that even when a bank is the victim of financial crime, of fraud, its tendency is to keep it inside and not to allow it to be known or to share information with other bodies for the purpose of coordinating efforts to prevent crime. I think it's important that financial institutions do co-operate for that purpose.

I probably have only a minute or so left in this round. Maybe we'll return to this, but I'll switch it a bit and quickly ask Mr. Hill about the processes that he referred to.

You talked about training and updating to meet changes to PIPEDA. How onerous do you think it will be to react to the new changes, for the mandatory reporting and whatnot? Is this going to be an onerous effort or not?

**Mr. Wally Hill:** I don't want to use the word “onerous”, but there is a job to be done, and to do it properly, organizations, especially large organizations, are going to have to change their processes and develop training to make sure that the appropriate staff are properly trained to handle the breach protocols.

We don't know yet what those will look like in detail. The discussions on what they might look like have been ongoing over the last year or so, with government officials, trying to ensure that they aren't unduly onerous in terms of some of the provisions. The law did require record-keeping and so on, and there is a question as to what degree of record-keeping organizations are going to have to work on.

**Mr. Pat Kelly:** Thank you.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much.

With that, we move to Ms. Trudel.

[*Translation*]

**Ms. Karine Trudel (Jonquière, NDP):** Thank you very much for your presentation.

I sympathize with my colleague. I would have made the same decision about the teddy bears. You made the right decision.

With social and peer pressure, I have unfortunately had to adapt to the digital era, to tablets and games, since I am a mother of two young boys.

I have done research on consent. I have noticed that parents put photos of their children on social networks and talk about their activities. I educate my young boys a lot about the importance of not posting just anything on those networks. There is a lot of educating to be done in that area, and it is our responsibility as parents. Unfortunately, we may miss some things.

I read that businesses may be forced to remove personal information posted on the Internet. It was said earlier that the processing of complaints would be a burden for businesses. If I have understood correctly, forcing businesses to remove personal information has to do with the right to be forgotten.

I don't know whether you are aware of this, but California passed a law on that issue, and I would like us to discuss it further. The law is titled Privacy Rights for California Minors in the Digital World, and it requires companies, websites and application designers to give children under the age of 18 an opportunity to delete information they themselves have posted. However, that piece of legislation does not pertain to information others have posted about minors.

What do you think about that? Could we apply the same principles here, in Canada?

[*English*]

**Mr. Wally Hill:** I think that could be challenging in terms of who we're defining as children. The users of social media, as you pointed out at the outset, are very wide-ranging. You have younger children and then you have teens who spend a great deal of time on social media. I'm not sure how some of those users, or their parents for that matter, would react to organizations arbitrarily removing information that has been posted by those individuals.

I have to say that I'm not familiar with the law or code you're referring to, so I'm just opining in a general sense. I think when you're talking about children under the age of 13, it's more challenging. I think that's the reason why social media networks have age limits and that type of thing. As I was saying earlier, our own code requires parental express consent, and even for children between the ages of 13 and 16 the consent of both parent and teen. Then it goes up in terms of gradients. I think it would be challenging to implement something along the lines of what you've described if it's across the board in terms of children and teenagers.

David, I don't know if you're familiar with that.

● (1615)

**Mr. David Elder (Special Digital Privacy Counsel, Canadian Marketing Association):** I'm certainly not an expert in California law, but I would point out that currently under PIPEDA, and under the principles at the end, there's a general right to withdraw consent for the use of any personal information, subject to contractual or legal restrictions. I would think that in a situation where someone had posted something themselves and wanted it removed, and there was no other valid contractual or legal reason an organization should keep or post it, in many cases PIPEDA would now require that it be removed.

I think a lot of social networks actually do operate this way. If you post something to a lot of social networks, you can remove it after you've posted it. It doesn't change the fact that people have seen it, and in some cases might not change the fact that others have copied it and distributed it in other ways, but you can pull it off the actual network it's on.

**Mr. Robert Ghiz:** I can understand where you're coming from. I have a four-, six-, and eight-year-old, and they are on their smart tablets, all the time. They're better at it than I am. We use it for teaching as well as fun.

As I said, when I was growing up, if I was going to get disciplined I'd probably get the wooden spoon. You're not allowed to do that now. We threaten to take away their smart phone and it's devastating for them. It's a good way to get them to listen to us.

**Voices:** Oh, oh!

**Mr. Robert Ghiz:** I'm not sure about the California law, but I'd be willing to get my association to look into it. I think there's also the component today of education. I know that the commissioner does fund such organizations as MediaSmarts, and there are other literacy things we need to do to make sure our kids today are ready for the realities of the world they're coming into. It's different from when we grew up. There is a responsibility to make sure that we educate kids that this is the new reality of the world.

For our members, there are rules and data management tools. The carriers have privacy settings on their phones. Parents need to be educated too, to help educate their kids, but I think we can start with young kids, telling them that these are the new realities of the world, and if they're going to be involved, there are associated consequences.

At any rate, I'd be willing to check out the California law. I understand where you're coming from, but I think there is a literacy and educational component to it as well.

**Ms. Karine Trudel:** Thank you.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** For our final seven-minute round, we have Mr. Saini.

**Mr. Raj Saini:** Thank you very much, all of you, for coming here.

I'll start with specific questions, and then I'll get to something a little bit more general. Let me start with Ms. Routledge and Mr. Docherty first.

As part of the CBA's submission to the OPC's consultation on consent under PIPEDA, you said that PIPEDA should not "pose a barrier to innovation". Can you explain what you meant by this? Do you feel that the way PIPEDA is currently structured poses a barrier to innovation?

**Mr. Charles Docherty:** As reflected in my colleague's remarks at the outset, we do agree that PIPEDA has served Canadian society very well up until now. Its broad-based principles are fairly technology-neutral. But as new products and new services are developed, it could benefit from some tweaks, in particular the concept of legitimate business interests so that privacy notices can be streamlined and people can really focus in on things that matter to them, that are meaningful to them.

I think that's what we were talking about in that submission.

● (1620)

**Mr. Raj Saini:** Mr. Ghiz, do you believe PIPEDA is a barrier to innovation?

**Mr. Robert Ghiz:** We're actually in agreement with the CBA. We think as new products develop—as we discussed with the 5G and the automated cars—there are provisions within the consultative process, and with the good relationship we have with the commissioner, we can work with the commissioner along the way to make sure we're ahead of the curve rather than companies making a mistake and then having to retract.

I view it as being more proactive, and I think there are mechanisms within PIPEDA to be able to do that.

**Mr. Raj Saini:** Mr. Hill.

**Mr. Wally Hill:** It's very much supportive of innovation. The way PIPEDA is now framed, it's designed for the kind of collaboration that is needed on a wide range of the innovative activity happening out there. To try to create a prescriptive law that deals with all the different areas that are evolving out there will just not be possible. That's why the law was framed the way it was. That's why it works so well and will continue to work well.

**Mr. Raj Saini:** Just to follow up on that, in the CMA's brief to the Privacy Commissioner, your group mentioned that the current EU framework as well as the new GDPR offer ways to process data without necessarily seeking consent each and every time. Can you expand on that a bit?

**Mr. Wally Hill:** I don't know that we were touching on the GDPR in our brief, but we were suggesting that it is challenging. Obtaining consent in the world in which we're operating today is indeed a challenge. We have touchpoints every day where individuals and organizations are asking us if we've read the privacy policy. We're dealing with small screens. There are enormous barriers out there to enabling consent in every interaction we have.

The point we're making is that you can retain consent at the core of your privacy framework and at the same time provide greater responsibility and accountability for organizations to utilize personal information where there is maybe a reasonable expectation on the part of the consumer that the information may be used for an additional purpose—in other words, an expanded use of implied consent, if you will. I think the CRTC was here a few days ago talking to you about the anti-spam law. A very robust aspect of that law is built on implied consent as well as express consent. There's a strong element of implied consent where there's an existing customer relationship.

Charles was talking about the fact that organizations may have a legitimate need to use the information for a new purpose that will not put the consumer at risk. It may indeed benefit the customer. In those kinds of instances, going back to consent, is that where we want to be in the environment in which we're operating today, the digital environment? We would suggest that it isn't, and that in different contexts, different industries, you may have different codes and different frameworks that will be established to allow organizations to move forward in the way that I've suggested. Those would be self-regulatory codes, and we think they have a place in what we're describing—that is, a consent-based regime still, but one that imposes great accountability on organizations.

**Mr. Raj Saini:** In some of your submissions and in some of your preambles, you also mentioned data breach notification and how you wanted that to be self-regulating. Can you enlighten the committee on why it would be an advantage for that to be self-regulating as opposed to mandatory?

**Mr. Wally Hill:** We're satisfied with the regulatory approach to a breach. It was originally a self-regulatory regime. The self-regulatory regime was built as a result of consultation. It was actually a great example of the kind of collaboration the PIPEDA model affords.

As data breaches became more of an issue through the last five or 10 years, the Privacy Commissioner and others recognized—I don't think there was disagreement within the business community—that there was more of a need to raise the bar and have a formal set of reporting requirements. Certainly the Canadian Marketing Association supports the breach notification provisions that are in PIPEDA now as a result of the amendments. We're engaged in talking to government about what the detailed regulations will look like just to ensure that they're not overly and unnecessarily burdensome to businesses and other organizations. That's our position.

● (1625)

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** With that, we'll have Mr. Kelly begin our five-minute round.

**Mr. Pat Kelly:** Thank you.

I am going to just pick up right where we left off, if you don't mind, and I'll let you have a little more of a complete answer than time permitted. We talked about compliance, and in your answer you talked about it perhaps being particularly an issue for large organizations.

I kind of thought about it the other way around, from the perspective of somebody who was once the operator of a very small enterprise. The smaller the enterprise, really, the bigger the burden of any kind of compliance and administration as a percentage of the organization. Do you not think that for any organization that has to comply with regulations, if the regulations are onerous, detailed, or large...? Do you think your smaller operators are concerned about compliance?

**Mr. Wally Hill:** For sure, smaller organizations are challenged. Everything you say is true. Proportionally, it can challenge smaller organizations, but I think they will move forward.

A lot of education needs to flow regarding things like the breach notification requirements of PIPEDA. Again, this is one of the reasons we have our current framework, with the ombudsman model and the Privacy Commissioner, as an advocate and educator, getting out there to these communities and ensuring that they're up to speed.

**Mr. Pat Kelly:** Does the commission do a good job on the education portion?

**Mr. Wally Hill:** I think they could always do more, but I think they do a pretty good job. They have tools for small businesses on their website, so I think they do try and they do a pretty good job. Could they do more? There's always more needed, as well as working with organizations like ours, the chambers, the Retail Council, and so on. Reaching out to smaller businesses and medium-sized businesses is always beneficial. That takes time.

**Mr. Pat Kelly:** In your opening remarks, you spoke about a risk assessment approach as differentiated from the consent model.

**Mr. Wally Hill:** It wasn't really to differentiate. It was to point out, for example, how the new breach requirements revolve around the concept of organizations reporting a breach where there is a real risk of significant harm, organizations having to make a judgment, and imposing that accountability on organizations.

I thought that term might catch people's attention if they were wondering whether they should be out there taking more risk.

No, it's that organizations should have imposed on them the requirement to evaluate the risk that is involved in the use of any information and to make appropriate decisions based on that. That's embedded in PIPEDA now, in the sections that deal with consent. There's a higher standard of consent required when you're talking about sensitive information as well as with the new breach requirements. There's a burden placed on organizations to make proper judgments as to the risk posed to consumers or customers with respect to some data that may have been leaked.

● (1630)

**Mr. Pat Kelly:** What do you think about having greater emphasis on this risk assessment? Do you want to tell us right now what kind of information you think is the highest risk and what is low risk?

**Mr. Wally Hill:** Typically high-risk and sensitive information certainly includes financial information or types of health information. Various categories of information are sensitive. Children's information by definition, because of the group in that instance, can be sensitive. I think it depends on context. The kind of model we're talking about is going to involve different approaches in different sectors.

**Mr. Pat Kelly:** Would it also help to update the definition of "publicly available"?

**Mr. Wally Hill:** I think it would. It may be possible to do that in the context of the existing regulations, I believe. PIPEDA does have regulation-making powers for the government. The Privacy Commissioner can seek to have regulatory changes that would help in that regard.

Go ahead, David.

**Mr. David Elder:** If I may just add to that, as a very specific example within the regulations now for "publicly available", one of the categories talks about how if it's "published", and it gives examples of being published in a newspaper or a magazine or things like that.

We've had several interpretations out of various privacy commissioners' offices across the country that say you can publish a blog every day and have 50,000 readers, but that anything you publish on that blog does not count as being publicly available for the purpose of the regulation. I think, in fact, there's room within that wording to say that "published" includes a blog.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much.

With that, we'll move to Mr. Dubourg.

[*Translation*]

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

Good afternoon, everyone. It is my turn to welcome you here.

I would like to begin with the representatives of the Canadian Bankers Association.

On page 3 of your presentation, you suggest that we improve the definition of "publicly available information". You said that, as that definition reflects the context of the 2000s and technology has since evolved, the definition should perhaps be rethought and modernized.

Can you elaborate on how we should modernize that definition?

[*English*]

**Ms. Linda Routledge:** As Mr. Elder just suggested, some of it is very paper-based. To amend it to allow for publication, not only with regard to blogs but if somebody is voluntarily putting information someplace else, would be helpful.

[*Translation*]

**Mr. Emmanuel Dubourg:** Earlier, you answered several questions from my colleague Pat Kelly about the definition of the term "financial crime" compared with the definition of the term "fraud". You said that the use of the term "financial crime" would allow for more information sharing among banks. So I assume that you regularly share that information with any branch or any bank. Is that indeed the case?

[*English*]

**Mr. Charles Docherty:** The circumstances under which information is exchanged without knowledge or consent are highly prescribed in PIPEDA. The banks take that obligation very seriously.

To your direct question, if they meet the requirements of the act, then they would share the information amongst each other, all with a view to combatting crime, which is an extremely important endeavour. It's meant to protect Canadians and the financial system as a whole, so they take that responsibility seriously.

[*Translation*]

**Mr. Emmanuel Dubourg:** I would also like to put a question to Mr. Ghiz.

You talked about the collaborative approach. Does that mean you would like penalties to disappear? Do you think that the collaborative approach should continue? Mr. Hill talked a lot about voluntary compliance with the legislation and so on. I would like to know what you think about penalties and then find out whether Mr. Hill agrees.

● (1635)

[*English*]

**Mr. Robert Ghiz:** We think the current penalties that exist now are the best way to go. We don't think there's any point in adding fines or extra powers. We say this because we've talked about the trustworthiness in all of our businesses, for everyone out there, and if you are going to be sanctioned or listed as someone who has made a mistake, the penalties that exist just in the public shaming alone are greater than anything any fine could do.

By putting the fine system in place, you're going to create a conflict, or it's going to become a bit adversarial. We're talking about the evolution of a lot that happens, whether or not it's autonomous cars, and working with the commissioner. We want to try to keep that collaborative relationship because we think that's what the sense of the act originally was.

**Mr. Emmanuel Dubourg:** Mr. Hill talked about negative publicity also. Is that your point of view?

**Mr. Wally Hill:** Certainly negative publicity, the impact with customers, and all of these things are incentives to compliance. I'd also point out that the commissioner does have other powers, as I mentioned in the submission. The commissioner, to make an important point, can go to the Federal Court. However, to change the order-making powers or the fining powers that the commissioner has, you have to create a different structure, and that will destroy, really, the collaborative, engaged approach that has existed for the past decade and a half and that has proven to be very valuable.

David, I don't know if you have anything perhaps to add on what would—

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** It would be great to have more comment, but unfortunately we're at the end of the five-minute round for Mr. Dubourg.

Mr. Kelly, you have five minutes.

**Mr. Pat Kelly:** The good news is that you can probably carry on right where you left off, because I would like each of the three organizations to weigh in on the following question. If I've understood your remarks correctly, all three organizations are rather down on the idea of order-making powers in PIPEDA.

There are privacy advocates who would disagree and would say that the ombudsman model and the collaborative approach that have been described are rather too cozy, and they would rather see the commissioner have more teeth. I'd like each of you to make your best and strongest case for the continuation of an ombudsman model rather than for order-making.

**Mr. Wally Hill:** You observed that people come forward and make the case, but they seldom point to glaring examples of where it isn't working. In my submission I tried to talk about all of the successes of the current structure, the collaborative structure that has existed in the ombudsman model to develop guidelines with the commissioner's office, the breach guidelines that were in place for seven or eight years, developed in collaboration with civil society, stakeholders, businesses, and others.

The AdChoices program to address the collection of data online when people are browsing is a self-regulatory program that our sector, the marketing and communications sector, developed in collaboration, to some extent, with the Privacy Commissioner's office. There have been a lot of great successes with protecting individuals' privacy and providing them with choice.

David, you may have a more legal response to this question about changing the model.

**Mr. David Elder:** I think when you're talking about order-making powers as distinct from penalties, which I think is a bit of a different argument, it really does come to that point. It's about collaboration. I'm here today representing the CMA, but I'm in private practice and I have other clients. I very seldom or never would suggest that someone go forward proactively to a government agency or regulator that has the power to fine somebody directly. If you did so, you'd be very circumspect in what you would say to them.

● (1640)

**Mr. Pat Kelly:** Understood.

I'm going to just make sure I let the others weigh in on this.

**Mr. Robert Ghiz:** We're quite similar, and as I mentioned before, I think for our industry, if you give more powers or if you give the fining authority, that's going to take away that working relationship.

As I said, reputational harm on an industry that relies on trustworthiness is really the most important thing to our industry. I think you're going to take away that relationship to collaborate by introducing more powers.

**Mr. Pat Kelly:** Okay.

Ms. Routledge.

**Ms. Linda Routledge:** We currently have a very good relationship with the Privacy Commissioner. We meet with them regularly to discuss issues. I think their role is to encourage compliance with PIPEDA and to facilitate that and to help give us the tools to allow us to comply with PIPEDA.

The evidence is there. There are very few complaints about compliance, and as Wally said, the outcome of these complaints is largely resolved with no problem. If that's the case, why is there a need for further enforcement powers?

**Mr. Robert Ghiz:** Could I add to that? For example, we have 30 million wireless customers, and there were 45 or 47 complaints last year. Out of those, the vast majority were done through early resolution.

**Mr. Pat Kelly:** Would it seem to you, then, that those who wish for order-making power are seeking to fix something that's not broken?

**Mr. Robert Ghiz:** I've sat in your chair for a long time. There are always people who believe that there should be more regulations put on more regulations, and sometimes, yes, if it's not broken, why fix it?

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** With that, thanks very much, Mr. Kelly.

We have Mr. Ehsassi in our final five-minute round.

**Mr. Ali Ehsassi (Willowdale, Lib.):** Thank you, Mr. Chair.

On this question, there has been very fascinating testimony from all of our witnesses. Thank you. It's been very helpful.

My question is for Mr. Ghiz.

As you know, the Privacy Commissioner believes that, given the transformative nature of the industries we're dealing with, consent is one of those significant issues that warrant attention and focus as we attempt to update the legislation. So far, I think you're saying that you don't see any need for revisiting the issue of consent.

**Mr. Robert Ghiz:** We think the current model is working. On consent, we said that we could look to evolve it into a broader sense. I think other witnesses here have talked about it today, how consent can be used more broadly to help it evolve with the new products that come to the forefront because of new technology and new products.

**Mr. Ali Ehsassi:** What specifically does that mean? Does that mean you believe in the concept of "meaningful consent" or not?

**Mr. Robert Ghiz:** We believe in the concept that there could be a better model around the consent so that it could help alleviate some of the regulatory burden.

For example, if we were to come out with a new product, we would need to change around all of our consent forms based on that, whereas we could create a consent model that could undertake to factor in new products that may come into the marketplace. Obviously, we've seen this in Europe. They're a little broader than we are. We don't have to look to reinvent the wheel. We can look to see where there are instances that we would agree with.

That would be one area where we would look for a change in consent.

**Mr. Ali Ehsassi:** Revisiting the issue of the right to be forgotten, you agree that's a significant challenge as well.

**Mr. Robert Ghiz:** I do.

**Mr. Ali Ehsassi:** However, you're still saying that whatever changes are made to deal with that issue, such as the changes that have been introduced by the EU and will be taking effect next year, they're too burdensome, correct?

**Mr. Robert Ghiz:** Exactly.

**Mr. Ali Ehsassi:** What would you consider to be something less than unduly burdensome?

**Mr. Robert Ghiz:** That's an open-ended question.

I would like to see the status quo, from our perspective, with the CWTA, but again, you see a new law in California that relates to things and you see other jurisdictions moving in directions.... I would say, first of all, that we don't believe there should be any changes, but for anything that would happen, I would like to see a consultative process.

We want to avoid a couple of things. One is the regulatory burden it could have on companies and businesses in Canada, which could perhaps slow down innovation. We also want to make sure that for any changes that come into effect, you will see level playing fields between Canadian companies and companies that are not Canadian and operate within our market.

● (1645)

**Mr. Ali Ehsassi:** Then what you're saying is that given that the EU is introducing change, and since you're in favour of a level playing field, that obviously would give us—operators here—a huge advantage, correct?.

**Mr. Robert Ghiz:** Under our rules that we don't want to change, yes.

**Mr. Ali Ehsassi:** Okay.

I will ask the Canadian Marketing Association a question as well. Thank you for your testimony.

Do you have any officials who focus just on PIPEDA? How does it work? Do you have outside counsel that deals with PIPEDA-related issues?

**Mr. Wally Hill:** Within the staff of the organization, within our advocacy team, we have people who focus on the issue of privacy. As well, we have our own privacy officer within our organization to make sure that we ourselves are doing things. Of course, we also have outside counsel, through David here, advising us on privacy issues, especially those related to the digital developments.

**Mr. Ali Ehsassi:** How do you monitor new technologies, or new marketing opportunities and things of that nature, which are constantly evolving?

**Mr. Wally Hill:** In much the same way you would in terms of following the literature out there and what's happening.... We also have marketing councils that deal with a variety. There's a digital marketing council, a branding council, and so on. Those councils are following very closely the changing technologies and trends within the various disciplines of marketing, so it's through mechanisms like that within the association.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much. That concludes our five-minute round. Now we have a three or three and a half minute round for Ms. Trudel.

[*Translation*]

**Ms. Karine Trudel:** Thank you.

Mr. Ghiz, you talked about the European agreement and about what is happening with the legislation. What good practices could Canada adopt? What would be the things not to do with regard to the bill we are considering?

[*English*]

**Mr. Robert Ghiz:** It's a good question. I remember when I was going through my remarks, I was saying to my staff that if I were sitting on the other side of the table, I would look for an area where I agreed with Europe and another one where I don't, and then call me hypocritical.

I also believe you don't always need to reinvent the wheel, so you can look at good things where they happen. Obviously, on the "forgotten" rule, we don't like what's happening in Europe. Around consent, we think they have a better consent model than ours. Those would be two that I would see there.

**Mr. Wally Hill:** They have, to some extent, a more stringent consent model. We would suggest it's not as innovation friendly, for example.

On the GDPR, the comment I would want to make is that adequacy is not the same as being identical. It would be premature for Canada to move to make changes to our privacy law before having consulted with Europeans going through the process. If need be, if they review Canadian law adequacy, then so be it. Let's see if any issues surface.

Quite frankly, Canada has one of the best privacy protection regimes in the world. It may be different from the the one in Europe, but we don't need to take second place and feel that our law is second to anywhere else in the world. I would strongly suggest that while the GDPR is very important for us all to be watching. It applies to business there. Let's see if they have issues with the adequacy of our law before we rush to make changes based on the GDPR.

● (1650)

**Mr. Robert Ghiz:** Just to be a little more clear, it's around their legitimate business interests. They allow more innovation than we would here. That would be the change that I would advocate for.

[*Translation*]

**Ms. Karine Trudel:** You just talked about personal information. Do you have any comments or recommendations about the retention and disposal of personal information?

[*English*]

**Mr. Wally Hill:** I'm not an expert in that field, but PIPEDA does impose very clear responsibilities on organizations with regard to the securing of information, safeguarding information, and proper destruction of information when it is no longer needed. That varies in terms of how long you have to retain information, the level of sensitivity, and so on.

Again, it depends very much on context, the industry, and the sensitivity of the information. That is why PIPEDA is based on 10 principles and has the flexibility to apply differently to different contexts.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thank you very much, Mr. Hill.

That concludes our formal question round. We do obviously have some time left on the clock if other members have questions.

Is it all right if I ask...? I have three questions, and I'll be quick.

My first question is this, Mr. Elder. Jennifer Stoddart was the Privacy Commissioner for 10 years. On the first review of the act, she did not recommend new powers for the Privacy Commissioner, but on the second review of the act, in her 10th year, she did. I'd also mention that she's a member of the Order of Canada. She said in 2013:

> We have made use of the existing tools under the Act, and in some cases, we have been successful in prompting change—but often after we have invested significant resources and almost always after the fact. We have seen some organizations ignore our recommendations until the matter goes to Court; others, in the name of consultation with the Office, pay lip service to our concerns but ultimately ignore our advice. There is nothing in the law that provides enough incentive for organizations to invest in privacy in significant ways given that they can always renege on their agreement to change their practices and decide not to follow through with the Commissioner's recommendations after the investigation or audit.
>
> The days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise.

Then she goes on to note that several provincial commissioners and international commissioners not only have order-making powers but fine-making powers, including in the U.K., Spain, New Zealand, and of course a number of provinces within our own country.

To put it more specifically, or more directly, why is Ms. Stoddart wrong?

**Mr. David Elder:** Far be it for me to say that Ms. Stoddart would be wrong. What I would offer is that we would take a contrary opinion.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** You must be a lawyer.

**Mr. David Elder:** Yes.

I mean, certainly there may be cases where organizations would not follow recommendations, and may not agree with the recommendations or the findings that the Privacy Commissioner may make, as is their right to do. Ultimately, the way the act is structured, the way it's supposed to be resolved, is that the matter gets brought before the Federal Court. The Federal Court, and the judges thereon, will look at it anew and come to a determination whether the statute was breached or not. That mechanism is already there.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Despite Ms. Stoddart's concerns, the Federal Court appeal mechanism is sufficient in your view.

**Mr. David Elder:** I think it is. From her perspective, it's more difficult to go through that hoop, rather than just to impose a fine directly, so I suspect that's where that motivation comes from.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Okay. I'll put my second question to Mr. Ghiz. We had a privacy expert, a downtown Toronto lawyer who practises law under PIPEDA, come to us and say that over 60% of 13- to 17-year-olds have at least one profile on a social networking site, and the right of erasure should be enacted in relation to minors where their personal information is collected. So it's not a right to be forgotten exactly in accordance with the EU perhaps, but it certainly seems like a fair recommendation. What do you think?

**Mr. Robert Ghiz:** I think a lot of people have those opinions and I think we are constantly changing, but I think we need to be very careful in terms of what we do. You have European law, you have California law, and there are other laws out there.

We worry about the burdensomeness of it and believe that we need to look toward the education component that exists with parents, but also with governments, the commissioner, and the kids involved.

● (1655)

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much.

My last question is for Mr. Hill. You had said—and I might misquote you a little bit—that there are enormous barriers to enabling consent, and that you were looking at perhaps a framework where there would be reasonable expectation that there would be additional purposes. Implied consent would expand perhaps where that new purpose does not put the consumer at risk or might in fact benefit the customer.

Just so I have some clarity, you're not talking about secondary marketing purposes, though, are you?

**Mr. Wally Hill:** No, not necessarily secondary marketing purposes. It could be any. It could be a situation where an app that's been developed, that is based on the use of personal information, develops a new aspect to it—

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** I'm sorry, maybe I phrased the question poorly. Do you think that there could be a situation where there would be implied consent for secondary marketing purposes?

**Mr. Wally Hill:** Yes, I think there is. For example, PIPEDA provided for the situation where, when a subscription to a magazine is expiring, organizations would be following up and remarketing that magazine to individuals. I think it is possible. I wasn't thinking particularly of secondary marketing. I was talking about, in a global sense, all kinds of possible situations.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** That marketing would be in relation to where there is an existing customer.

Would it not be in relation to sharing or selling that information to third parties?

**Mr. Wally Hill:** No, not sharing the information with third parties, except in situations where third parties are providing a service to the organization.

I think when you're sharing information, you need express consent.

**The Vice-Chair (Mr. Nathaniel Erskine-Smith):** Thanks very much.

Is there anyone else with questions?

With that, thanks to all for attending. The meeting is adjourned.