HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 063 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, June 1, 2017

Vice-Chair

Mr. Nathaniel Erskine-Smith

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 1, 2017

● (1530)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Welcome to the 63rd meeting of the Standing Committee on Access to Information, Privacy and Ethics.

We are continuing our study of PIPEDA.

Welcome to our witnesses from the Canadian Association of Research Libraries, the Association of Canadian Archivists, the Retail Council of Canada, and Google Canada.

We will begin with presentations of 10 minutes each, followed by questions.

We'll begin with Ms. Bourne-Tyson and Ms. Haigh from the Canadian Association of Research Libraries.

Ms. Donna Bourne-Tyson (President, Canadian Association of Research Libraries): Good afternoon.

Thank you for the opportunity to speak to the Standing Committee on Access to Information, Privacy and Ethics during your hearings on the Personal Information Protection and Electronic Documents Act.

My name is Donna Bourne-Tyson. I am the university librarian at Dalhousie University; president of the Canadian Association of Research Libraries, known as CARL; and a board member of the Canadian Federation of Library Associations. Joining me today is Susan Haigh, executive director of CARL. We are pleased to be here to share the research library perspective on the right to be forgotten.

CARL is the national voice of Canada's 31 largest research libraries, 29 of which are located in Canada's most research-intensive universities. CARL also represents Canada's National Science Library and Library and Archives Canada. CARL members' parent universities attract over $6 billion in research funding annually, and our member libraries spend over $285 million annually on information resources to support learning, teaching, and research.

CARL members act as a foundation for Canadian-led innovation by providing access to knowledge as well as preserving vital information required to support Canada's research community. Academic research libraries are at the vanguard of technology as the sharing and dissemination of information shifts to digital environments. In this light, CARL has watched the emergence of the right to be forgotten with great interest.

Our position is that there are important rights and freedoms to be weighed, respected, and judiciously balanced in any legislation or regulatory approach to the right to be forgotten. As we noted in our short submission to this committee in April, we are guided by the "Statement on the Right to be Forgotten" issued by the International Federation of Library Associations, IFLA, in February 2016.

CARL has elected to focus comments on the right to be forgotten, but we do support the perspectives on PIPEDA more broadly that will be outlined today by our colleagues from the archival community. Research libraries play an increasing role in research data management, and we are very engaged in defining and practising what we might call the ethical management of data. The library and archival communities see data management as key to ensuring appropriate protection of individual privacy while, at the same time, enabling more data to be openly accessible and allowing technology-based research that mines anonymized or aggregated datasets.

Now I will turn to our views on the right to be forgotten.

In 1987, CARL adopted a freedom of expression statement that confers responsibility on Canadian research libraries to "facilitate access to...expressions of knowledge, opinion, intellectual activity and creativity from all periods of history to the current era including those which some may consider unconventional, unpopular, unorthodox or unacceptable". This statement echoes the fundamental right to expressions of knowledge, creativity, and intellectual activities as embodied in the Canadian Charter of Rights and Freedoms.

At first reading, the right to be forgotten appears to run counter to this responsibility. This is not to say that libraries do not believe in protecting the right to privacy. Rather, as I will discuss here, the right to be forgotten is a complex, emerging, ethical and technological issue that demands a careful balancing of fundamental rights that, at times, can appear to be in conflict.

Libraries are, by their very mission, upholders of the public interest and are sensitive to the concerns around personal privacy on the Internet. The library community recognizes that information on the Internet can cause harm, particularly in cases where the information is false or defamatory. The right to be forgotten can be a legitimate means for individuals to address these situations.

Libraries are also the preservers of the public record and defenders of freedom of speech and access to information. The research library community has identified three dangers to be avoided by any legislation or regulatory approach to the right to be forgotten.

First of all, privacy, however important, must always be weighed against other rights, such as freedom of access to information and freedom of expression. These freedoms are not honoured when information is removed from access or is destroyed. While content can be removed from the Internet by its owners, a "right to be forgotten" approach must ensure that the privacy rights of an individual who is the subject of the content do not unduly impinge on the expression rights of creators of the content, such as authors and publishers.

Another danger of the right to be forgotten is the potential for the over-removal of content. If a right to be forgotten is encoded in PIPEDA or another piece of legislation, lawmakers and/or regulators must be proactive in reducing the incentives of platforms like Google or Facebook to simply delist information upon any request. In the section of its transparency report that addresses "right to be forgotten" search removals in Europe, which is accurate up to May 28, 2017, Google has evaluated over two million URLs for removal, with 750,487 URLs removed.

● (1535)

While Google does appear to be attempting to balance competing public interest in its decisions, it is important to remember that for each time an individual's privacy is protected through a right-to-be-forgotten request, it may muffle the speech of those whose content is being delisted, raising the spectre of censorship.

Another closely related issue is the integrity of the historical record. Information on the Internet may have future value, both for the public and for researchers. We believe an expert assessment of the impact on the historical record, preserved for future generations of Canadians, and ways to mitigate that impact should form part of every decision to remove information. In recommending this, research librarians recognize that the digital age has increased the accessibility of historical records that might otherwise have persisted only in physical libraries or archival repositories.

In that light, an approach to the right to be forgotten that downplays visibility by suppressing access through search engines seems marginally more acceptable than outright removal. In effect, delisting removes information from the public view obtained through a simple keyword search, but does not actually remove it from the reach of the more skilled and persistent researcher, who may also search for repositories that are not indexed by search engines.

Therefore, in our view, a limited and nuanced application of the right to be forgotten is appropriate. The removal of links to references to a minor juvenile crime or to sexually explicit photographs of a private citizen are examples of a proper application of the right to be forgotten, but what of the removal of links to references to a business failure, an injudicious statement by a corporate CEO, or public records that have not been sealed by court order or judicial practice?

To cite a recent specific example, a request was made to remove from the Internet a thesis that contained a chapter relating to organized crime activities by a named person who had since changed his life. The request was not acceded to because it was determined that the work was valid research and because the request was not supported by the thesis author and copyright holder. In that example, CARL would say that the correct decision was made; the thesis should not have been removed from the Internet simply because the person did not want any references to his criminal past to be on record.

The right to be forgotten should not be able to be too casually invoked by individuals, or their requests too readily acceded to by search engines. If implemented, such a right must have limited application, with clarity as to the conditions under which it may apply. There are complex considerations to be weighed and rights to be balanced, very likely requiring case-by-case assessment. In most cases, a review by an informed, but impartial, party is essential. A right-to-be-forgotten regime that requires a judicial order for any information or data removal seems merited, rather than leaving companies like Google or indeed research libraries with the task of deciding on sensitive, ethical situations pertaining to individual Canadians.

In closing, CARL, on behalf of the research community that its library members serve, calls for a very constrained approach to the right to be forgotten, one that will generally require a judicial order, and will not apply where retaining the links in search engines is necessary for historical, statistical, or research purposes; for reasons of the public interest; or for the exercise of the right of freedom of expression.

Thank you.

● (1540)

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

Our next presentation will be from the Association of Canadian Archivists, and we have Mr. Kozak by video conference.

Mr. Greg Kozak (Representative, Ethics Committee, Association of Canadian Archivists): Good afternoon, and thank you for the opportunity to speak to the committee today. My name is Greg Kozak, and I'm here today speaking on behalf of the Association of Canadian Archivists. I am a professional records manager and I also teach as an adjunct professor at UBC's School of Library, Archival and Information Studies, focusing on access to information and privacy legislation.

The ACA is a national association of professionals who work in the public and private sectors. We have close to 500 individual members and 200 institutional members across the country. Our scope of interest spans the entire life cycle of records, both digital and physical, from their creation to their final disposition, whether that is destruction or permanent retention.

We're also advocates for consistent, accurate, and transparent information management practices that respect national and international standards. Our membership thus includes records managers who deal with current records within their organizations and archivists who deal primarily with historical records in archival institutions or programs. Sometimes, both responsibilities overlap.

We are interested in providing comments on existing or proposed legislative or regulatory texts that may affect our ability to manage trustworthy records and preserve, control, and provide access to authentic records over the long term. It is on these points that we would like to focus our remarks.

Trustworthy records are records that are created in a way that ensures accuracy, completeness, and reliability and that are then maintained and preserved so that their identity and integrity—their authenticity, that is—are unquestionable. Trustworthy records are records that can be used as evidence of the facts and acts that they attest were referred to for both legal and research purposes.

In our increasingly digital and connected world, keeping trustworthy records has become more complex. Much of this complexity relates to privacy issues and to the management of personal information.

Specifically, we see two areas related to privacy in which trustworthiness of a record is challenged. The first is the processing of the data in the creation and maintenance of records.

In his letter to the committee, the Privacy Commissioner of Canada stated that “it is no longer entirely clear who is processing our data and for what purposes”. To add to this point, we would like to note that we do not know how our data is being processed or by what means. The growth of visual analytics as a method of analysis and a reliance upon complex algorithms mining various datasets for decision-making result in a complex web of interactions whose outcome is likely to infringe on the privacy of the people whose information was collected.

In such situations, good records management is a prerequisite to the protection of privacy, as it would control the processing of the data of individuals while ensuring the creation of a reliable record of actions of those who are entrusted with them.

The second area in which trustworthiness of records is challenged is in the use of certain security measures to de-identify personal information contained in records. An example of this is tokenization, whereby a known individual's identity is replaced with another unique, non-obvious identifier. The controlling agency retains a table of concordance that permits it to match a unique identifier with the known individual.

The issue here is that such security measures are creating records that are difficult to manage over the long term. Again we can see a convergence between records management and the privacy requirements. In order to establish a level of trust over de-identified records, we still need to know what actions were performed on them.

Considering the challenges described above, it is clear that solid information management practices are a foundational element to effective privacy management. The ACA thus recommends that organizations be required to include records management capabilities within processes and systems that encompass privacy needs. This aligns with the direction of the European Union's general data protection regulation, which requires privacy by design and default; in other words, records systems designed with privacy in mind.

● (1545)

Our next comments deal with the preservation of records, which is the second hat that we wear.

Archivists acquire records that stand as testimony of human action. These records, created by public and private organizations and individuals, span all fields of endeavour—administrative, scientific, legal, financial, and cultural. Archives acquire records that show humanity at its best, its most ordinary, and its worst.

Preserving records is a societal good that ensures the historical accountability of one generation to another and permits the public to access unique sources of information for a broad range of purposes, such as historical research, scientific inquiry, and addressing past injustices through reconciliation efforts.

In this regard, we recommend preserving PIPEDA's existing mechanisms that permit private organizations to donate records containing personal information to archives for long-term preservation, allowing archival institutions or programs falling under PIPEDA to acquire records containing personal information, and carefully considering the implications of introducing a right to be forgotten or a right to erasure.

At the moment, PIPEDA permits organizations to donate records containing personal information of long-term value to an archival institution for preservation. This mechanism should be maintained to ensure archives are able to acquire and maintain records of private organizations. It is vital that private organizations be able to donate their records, to ensure the all-of-society representational nature of archival holdings.

One area where PIPEDA could be improved is allowing archival institutions covered by it to acquire records that fall under the archive's mandate. Currently, such archives need consent from the data subjects to acquire records containing personal information. In practice, it is very unlikely that organizations would seek consent to allow records containing personal information to be donated to a third party.

Therefore, the ACA recommends that archival preservation of records be recognized as consistent with the initial purpose for which personal information was collected. This reflects the approach adopted by the EU's regulations, where further processing for archival purposes is not considered to be incompatible with the initial purposes of collection. However, the organization must have a bona fide archival mission consistent with ACA's code of ethics and professional conduct, and not have been set up as an archives for the purposes of avoiding the act.

Third, the ACA believes that if a right to be forgotten or erasure were introduced, it would impact the ability of archives to preserve records. It is essential to ensure a careful balance between protection of an individual's reputation and the integrity and authenticity of the public record. PIPEDA is already based on the principle that personal information needs to be kept accurate, complete, and up to date. A wider application of this principle could help rectify instances where incorrect or inaccurate personal information may result in reputational harm, reducing the need for a right to be forgotten.

Regardless, the test to determine reputational harm must be clear, and the bar should be set high enough to remove frivolous or inconsequential requests.

We should also view such a right to be forgotten from a historical perspective. Specifically, it is to be considered that personal information becomes less sensitive over time. This is already acknowledged in PIPEDA, where it is established that information about someone who has been dead for more than 20 years, or in a record that is over 100 years old, can be disclosed freely.

Similarly, the EU's regulations do not apply to a deceased person. Therefore, reputational harm will diminish over time, and there will be a point when it causes no harm. Thus, the legislator should be mindful of introducing any measure that may irreversibly remove or conceal records.

I'll make one final comment on the application of cloud environments in privacy.

Increasingly, records are created, maintained, and preserved in cloud environments that are characterized by location independence. This type of environment was in fact the catalyst for the European data protection regulation, and is a strong aspect of the drive in several countries towards jurisdictional location requirements for the data related to their citizens.

● (1550)

In Canada, some provinces require that public bodies ensure that personal information under their care or control is stored and accessed only in Canada, subject to legislative exceptions. The Canadian government does not prohibit government institutions under the Privacy Act or organizations under PIPEDA from using cloud service providers that store personal information outside Canada but recommends that the privacy risk be identified, including the need for transparency, consent, and notification of the individual the personal information is about.

The ACA believes that PIPEDA should make a definite statement on the issue of the jurisdictional location of data of private individuals; otherwise, what happens to them will be mostly decided by legal opinion rather than by clear, consistent rules.

That concludes our submission. Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much for that presentation.

Our next presentation comes from the Retail Council of Canada.

Mr. McLinton, you have 10 minutes.

Mr. Jason McLinton (Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada): Thank you, Mr. Chair and esteemed members of the committee, for allowing us the opportunity to provide our comments on the review of PIPEDA from a retail perspective.

The Retail Council of Canada, RCC, has been the voice of retail in Canada since 1963. A not-for-profit, industry-funded association, we represent over 45,000 storefronts of all retail formats, including department, specialty, discount, and independent stores; grocers; and online merchants. Retail employs approximately 2.2 million Canadians, and as such is the largest private sector employer in the country.

I am the vice-president of the grocery division and regulatory affairs for RCC. This means that I am responsible for coordinating a range of regulatory files that impact retailers as sellers of products, as private label owners, or as employers. I manage files from food safety to consumer product safety, from drug labelling to regulatory co-operation. This includes matters such as anti-spam regulations, as well as digital privacy and security.

While we are not in a position to comment on the intricacies of PIPEDA, we are pleased to offer some general observations from a retail perspective. Generally speaking, in our view PIPEDA strikes the right balance between taking actions to protect digital privacy and taking a forward-thinking, technology-neutral approach.

As you know, a core concept in the legislation is that of consent. This is a very valid principle. We understand that the Office of the Privacy Commissioner held consultations on the issue and will be releasing a report later this year, and we would be pleased to participate in any consultations the commissioner may consider on guidance around valid consent.

Another core principle of PIPEDA is the mediator/conciliatory partner approach. This approach has a proven track record of working very well. In fact, our members have indicated that they can be and indeed are much more forthcoming in this context than they could be in a more formal, legal context. After all, we are all seeking the same goal: customer trust. Consumer trust is the core incentive to strong privacy protections, not expanded legislative powers and penalties.

RCC members are very aware of privacy issues and take their consumers' information very seriously. From our perspective, additional prescriptive requirements or enforcement powers would accomplish little in this regard, except to add to compliance costs.

RCC members spend a lot of time and effort trying to ensure that their systems are safe. However, the sophistication of hackers and scammers knows no limits and, despite best efforts, they will continue to find ways to circumvent the security systems that lawful businesses have put in place.

Unfortunately, it is easy to blame businesses that try to protect the information they have, because in most instances they can be located and the scammers cannot. Creating stricter requirements and broadening enforcement powers would unfortunately do little to change this situation, except to increase the cost of doing business in Canada.

RCC supports the current collaboration and communication between the Office of the Privacy Commissioner and provinces that have their own privacy legislation, and would hope that this continues as other jurisdictions consider legislating in this area. This would avoid the potential for uncoordinated and inconsistent reporting requirements.

Finally, it is important to remember that consumer data benefits consumers and Canadian businesses alike. Consumer data allows companies to understand what makes individual consumers tick and enables them to tailor and offer products that consumers may want to buy. It shows societal trends, which allows them to adapt their businesses and product offerings. It may indicate where bricks-and-mortar locations might be appropriate. It is useful for feedback on their business: where it went wrong and where it went right. Consumers can benefit through the steps companies take to improve the products they offer based on information they gather. Targeted advertising, when appropriately consented to, can reduce the time consumers spend looking for products by focusing on the things of most interest to them.

To conclude, retailers are supportive of PIPEDA and its technology-neutral approach. It has a proven track record.

Thank you again, Mr. Chair and members of the committee, for the opportunity to be here today.

● (1555)

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

We go to our final presentation. For up to 10 minutes, we have Google Canada, represented by Mr. McKay.

Mr. Colin McKay (Head, Public Policy and Government Relations, Google Canada): Thank you very much, Mr. Chair.

Members of the committee, thank you for the invitation to appear today to speak to you on such an important subject.

We, meaning Google and I, haven't had the opportunity to appear before this committee in quite a while, so I'd like to take a few brief moments to tell you about Google in Canada.

In 2002, Google opened its doors in Toronto. It was one of our first offices outside the United States. After 15 years of growth, we now have more than 1,000 Googlers working across four offices: in Toronto, Kitchener-Waterloo, Montreal, and right here in Ottawa. We are excited about Canada. We are excited about the way we've been able to build world-class engineering teams that work on products used by billions of people every day.

Those products are being worked on in the four offices I just mentioned. Our products are being used to map northern communities, to make national parks more accessible to all, and to make our morning commute as painless as possible.

We are also increasingly working with Canada's community of artificial intelligence and machine learning researchers in both Toronto and Montreal. Canada, as we all know, is a world leader in this field, and the opportunity for scientific breakthrough, practical innovation in consumer and business products, and industry-wide growth bodes well for the Canadian economy.

I will turn to the subject under discussion today, PIPEDA. I've been in this field for more than 10 years, and I've always debated how to say it, so I'm glad to hear that there's a mixture.

As a principles-based privacy framework, PIPEDA is as relevant today as when it was first introduced. The broad principles that underpin privacy and data protection regulation have held fast through many cycles of technological change. We expect that the same will hold true as we see mobile devices gain in popularity and as machine learning gains wider use.

Of course, the specific application of these privacy principles will change and evolve, as it always has. At Google, we believe that data-driven innovation is compatible with a commitment to privacy. Our commitment focuses on four elements.

The first is choice. We provide users with meaningful privacy choices throughout the lifespan of their Google account: when creating their account, as they use our services, and when they abandon or delete their account.

The second is transparency. We help users make good privacy decisions by making it easy to see what data Google collects to power the personalization of their services and the advertising they may see.

The third is control. We provide our users with powerful, meaningful privacy controls, ensuring that they are experiencing Google on their own terms.

Finally, and I would say importantly, comes security. We invest heavily in keeping users' data accessible to them and only to them.

At Google we know that there is no “one size fits all” approach to protecting user privacy. Privacy means different things to different people, and we want to help our users to feel comfortable and confident about the information they share with us, even as they interact with our products on desktop, tablet, phone, or home devices.

We place value on being upfront and transparent with our users and speaking to them about privacy in clear language that they understand. In 2015, we introduced a site, privacy.google.com, that answers some of our users' biggest questions, such as what data Google holds or collects and what we do with that data. We've also made users' settings easier to find, understand, and manage, putting it all together in one place called My Account.

I want to underline that while I'm listing websites and URLs, the effort that has been put into experimentation and user experience design to make these useful has been a decade-long investment and process of refinement.

We're not stopping there. We continue to innovate and to improve users' access and control over their account data. For example, we are giving users unprecedented transparency through a site called My Activity, where they can see and manage the information used by Google resources.

How are they reacting? There were 1.6 billion unique users to this My Account site in 2016, and importantly, for we all realize how we use devices and how we access the Internet nowadays, more than 50% of that traffic was from mobile devices. Users have questions about their privacy and their security, and they're getting those answers relatively easily on a device that is really quite small.

With a focus on data security and access control, reasonable user awareness and empowerment, and data portability, we—both Google and the industry writ large—can ensure both privacy and innovation. It's the misuse of data, not its collection, that should concern us most. Let's consider the application of machine learning and the use of algorithms.

These techniques are already deployed in many features that Google's users know and love, such as Google Translate, spell-checking, or spam filtering, and within products such as Gmail, for instance.

● (1600)

Those of you who use our email products may be familiar with something called Smart Reply, which is generated by machine learning and uses our latest neural nets to suggest short responses relevant to incoming email, like “sure, I'll jump on that” or “that looks good to me”. People use it for 10% of all replies in our mobile mail products, so when you see that next time you'll know it might not be that genuine.

Google Home, which is a stand-alone device that provides access to our services, is also screenless and voice-controlled. We had to think of a new way to deliver our privacy notice to users by designing a specific sign-up and user consent flow for this product using a Home mobile app, and to make users aware that they can access their privacy controls through their Google account. You've had conversations around this sort of subject in your previous meetings, and it is truly a complex area.

At Google, we feel well positioned as we transition to a new era of computing in which people will experience computing more naturally and seamlessly in the context of their lives, powered by intelligent assistance and the cloud. This transition is as significant as the move over the last decade from desktops to mobile devices.

I'll just touch on two specific points that came up in your previous meetings, and we can follow up in the questions, if you like. You've heard from several witnesses about the challenges of maintaining children's privacy online. We are acutely aware that all our users need to understand the technology they use every day. We invest in making information available to parents. Through tools like the Safety Center, Family Help Centers, and in-product notifications, we work to provide parents and families the information they need to guide decisions about their children's use of technology. We want to provide parents with the tools and information they need to make their own choices regarding their children's online activity. We have built features into our Family Link app, which at the moment is only available in the United States, and our YouTube Kids app to enable parents to decide what is right for their family. The goal is to give kids an experience, guided by their parents, where they can build the skills to engage in smart and responsible online practices as they grow as individuals.

Finally, you've asked previous witnesses, and you've heard from Ms. Bourne-Tyson, about Europe's right to be forgotten.

Information-finding services like search engines are critical for sifting through the vast amount of information online. Many have likened the ruling by the Court of Justice of the European Union to removing cards from a library card catalogue but leaving the books on the shelf. However, on the Internet there are no shelves to browse, no way to walk through the stacks and follow the alphabet to the information you seek. Decisions to delist URLs can affect users' access to media properties, past decisions by public figures, and information about many other topics.

Of course, we at Google understand that there are instances where it's appropriate to remove content from search results because, for example, it's been deemed illegal under local laws. Our products have well-established systems for users to flag content that violates our policies. Authorities may also submit requests to locally block content that is deemed illegal under local laws, including laws about privacy. We have worked hard to be a responsible actor. A crucial aspect—which has been mentioned already today—of this responsibility means balancing privacy with other values, specifically the right to free expression.

While the CJEU may have established a right to be forgotten in Europe under European laws, it is important to note that freedom of expression is a broadly recognized, and passionately defended, right here in Canada and across the Americas. Any framework that has such significant implications for the freedom of expression must be accompanied by transparency, accountability, and recourse mechanisms. And any discussion of the possible application of a right to be forgotten in Canada should recognize and address the complex dialogue around this issue that continues to exist today in Europe.

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

● (1605)

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

And thank you for the presentations from all witnesses.

We'll begin with Mr. Long for a seven-minute round.

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

Thank you to our witnesses this afternoon. They have been very interesting presentations.

Mr. McKay, I'm excited that you're here today. There's so much that we can wrap around with respect to Google, but I'm just going to leave you for one second.

I'm going to speak to Mr. McLinton.

You said that you represent 45,000 stores. You also said that you think there is the right balance in PIPEDA right now. Can you elaborate why you feel there's the right balance? With ever-changing technology.... I know you said it's technology-neutral. With the ever-changing technology we've had a lot of people telling us there should be amendments to PIPEDA because of the rapid change in technology.

Can you elaborate on this?

Mr. Jason McLinton: From a retail perspective, because the nature of retail is such a reputational one, the members that the Retail Council represent want their brand to be known, and of course, many of the members that we represent are very familiar household names. For them, the interest of protecting the privacy of their consumers is inherent in their business, as opposed to something that would be less technology neutral and more specific, that would not allow that kind of flexibility to adapt to change over time. They inherently already have that self-interest. It's a reputational issue, and they want to keep their consumers happy and coming back.

Mr. Wayne Long: Okay, you have 45,000 members. You obviously have some large retailers, and I'm sure, some very small mom-and-pop retailers. What are you doing, from the council's perspective, to make sure that they are up to speed, being educated, being informed, and are ready for the changes that are coming with respect to privacy?

Mr. Jason McLinton: Just to clarify, it's 45,000 storefronts, which would be approximately 2,000 to 3,000 members. From my estimation and the conversations I've had with the members, the level of awareness is already extremely high. Because of the self-interest and the need to protect their consumers' information and wanting to keep their consumers coming back, that level is already quite high.

Mr. Wayne Long: I respect that, but just from the Retail Council's perspective, are there any initiatives you have to make sure that members are up to speed?

Mr. Jason McLinton: For example, the Retail Council had a privacy committee where members would get together and share information and best practices around issues related to privacy. On Canada's anti-spam legislation, we held a number of webinars around that. So a number of activities are being held. We also have partnered with the Canadian Chamber of Commerce in doing some educational awareness activities around data breach reporting and things such as that.

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

I'll just shift to Mr. McKay; and Mr. McLinton, you might be able to chime in here too.

A common theme that I've talked about for the last several months has been the protection of children under PIPEDA. My own opinion is that there's not enough protection for children. If you look at COPA, the Child Online Protection Act in the States, it's quite explicit and I think much more defined with respect to children.

When I look at my friends who have younger kids, obviously they're on their pads and searching on Google, and they're using their emails, and so on and so forth. However, there's not a lot of control there.

I just had some people over last weekend at the house. They brought their younger kids, and they're obviously more aware of what's going on now. So I asked the parents, “What are they on? What are they doing?” They said, “Oh, I don't know.”

The concern that I have, and I think the whole committee has, is the protection of children. Mr. McKay, can you elaborate? Do you feel that children are being protected enough with respect to consent?

● (1610)

Mr. Colin McKay: I have three kids of my own, and I think a lot of the effort comes—

Mr. Wayne Long: How old are they?

Mr. Colin McKay: They've grown up with the Internet. They're ages 22, 21, and 17.

The focus has always been on being aware of what your children are doing, whether inside the house or outside the house, on a device or with friends, or possibly with a group of new friends. That's where we focused some of our efforts: explaining what those interactions look like online and providing tools for parents.

Mr. Wayne Long: You talked in your presentation about a Google family app. Can you elaborate on what that is?

Mr. Colin McKay: Family Link is in a beta-tester program right now. It was just launched in the United States. I think it tries to address some of the concerns you have, that in the context of a young child, how does a parent have some level of awareness and control over what the child is doing with online tools? It creates family profiles, including a profile for the child, that the parent can limit. The parent can limit the types of sites they can visit, limit the amount of time the child uses the devices. It can provide a record of what in fact they did visit and what they looked at so there can be that honest conversation among family members around how they're using devices and what they're seeing.

Mr. Wayne Long: Mr. McLinton, do you have anything to add to that?

Mr. Jason McLinton: I don't have very much to add.

Just to come back to the notion of consumer trust and business interest, from a retail perspective, it's not in a retailer's business interest to in any way compromise any age group, right? It's about keeping your consumers' privacy intact and giving the consumers what they want.

Mr. Wayne Long: Okay.

Mr. McKay, with respect to these children, I appreciate that your children are older; mine are too. Do you think there should be tiers, like maybe 14 to 16, or eight to 12? Should there be different types of consent for different age limits?

Mr. Colin McKay: There's a difficult question here, which is how exactly a company like Google or any other company would identify an individual to a level where they would then be certain to enforce those tiers. That's part of the challenge that COPPA presents, in that you don't want to create a record of someone who's under 13 years old, right? That's why we focus on the family unit and having authority figures recognize who in the family needs that level of influence and that level of control.

Mr. Wayne Long: Thank you very much.

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

Our next seven-minute round of questions goes to Mr. Jeneroux.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair, and thank you, everybody, for being here today.

I want to start with you, Mr. McKay, and dive a little bit deeper into the right to be forgotten. We've had a number of witnesses before us here at committee who've weighed in on it. We're waiting for the Privacy Commissioner to provide his fulsome analysis of it, but we're hoping to get as much from a variety of sources as we can, you being an obvious one.

When it comes to the right to be forgotten, or the right to erasure in some cases, how do we determine where and who should be forgotten? You mentioned elected officials. There have been a number of cases where I'm sure certain elected officials would like to have their pasts forgotten, none around this table, of course, but certain other ones. I feel that it's also imperative in certain cases that the public know what's out there.

I guess Google's approach to the right to be forgotten would be helpful to us when drafting our report.

Mr. Colin McKay: The right to be forgotten, as it's identified and implemented in Europe, is problematic because it effectively creates an administrative role for Google, as a private sector corporation, in deciding what information users can and cannot see, but it doesn't remove that information from the Internet. We're placed in the uncomfortable position of staffing up and running an office that then makes a decision about whether or not a request to delist a URL from search results is in fact appropriate, based on the laws of 21 different jurisdictions.

You're very right. As was mentioned by Ms. Bourne-Tyson, there are people who have childhood criminal records or were indiscreet in university, and then there are people who have explicit corruption convictions or other violent crimes, or more simply, who have a history of poorly stated and poorly thought out political or personal beliefs. It's a difficult role for the private sector to be the adjudicator on that.

● (1615)

Mr. Matt Jeneroux: The camera's on you.

Some hon. members: Oh, oh!

Mr. Colin McKay: Or it would be in the Canadian context. Part of the challenge is that this right has been created in lieu of having a serious civic conversation about when information should become opaque to users.

If we have a requirement for administrative decisions to be made public in a specific context, the right to be forgotten tries to create an end run around that by obscuring that information again, rather than having a fulsome conversation around whether there should be a time limit on making that administrative judicial information public, and around whether bankruptcies should have an expiry date in terms of publicity as well as relevance to your credit record.

That's why, in my admittedly short remarks, I made the observation about it needing a full dialogue. It's not just a question of a deliberation as an element of a possible revision to PIPEDA. It's actually a full dialogue around what we expect in a democratic society around free expression, the retention of records, and the retention of information about people in the context of both legal and public proceedings.

Mr. Matt Jeneroux: I appreciate that. In following the line of questioning of my colleague Mr. Long when he spoke specifically about kids, it's one thing to have set up a family link app. You mentioned it's not in Canada yet. It sounds interesting for that type of enforcement, but still that doesn't stop them from going to school and having another kid, who doesn't have that similar set-up, take a photo, upload it, and boom, it's part of the public record.

I want to shift a little to a witness we had here, Dr. Michael Geist. He brought up algorithmic transparency. He suggested that should require search engines and social media companies to disclose how information is used to determine the content displayed to each user. I'm curious about your thoughts on algorithmic transparency. Do you think it's feasible?

Mr. Colin McKay: We already try to provide that information to our users, in the context of that recitation of websites that I mentioned in my account, where underneath that you can see a record of your location history, your search history. You can see how we've made decisions around what advertising you should see, based on broad categorizations that are based on the search behaviour and ads you click on within our properties.

Rather than discussing algorithmic transparency, we need to focus on the outcome of that process. Does that outcome demand intervention or does it demand supervision? You have to have a measure of the levels of harm, and an idea if you're seeing outcomes that are detrimental to the individual.

It's difficult to say that algorithmic transparency, in being able to see outside the box and see the gears, will reveal anything. In many cases the inputs that are coming through the algorithm change are on a near-instantaneous basis, providing immediate results. Understanding both the information that's being collected, which is already a requirement under PIPEDA, and then understanding the outcomes is more relevant to the challenge we're trying to face, which is the individual user's understanding of their interaction with the box and the system, and then how that is influencing the information that's presented to them.

Mr. Matt Jeneroux: Do you keep certain algorithms private in, say, a competition place?

Mr. Colin McKay: Yes, they're all considered corporate assets. There's an example of when we were a young company and all we had was a search product. Larry and Sergey, our founders, published a paper about the page-ranking system upon which the search product was based. Just the process of publishing that paper gave spammers who wanted to game the search rankings and get a higher ranking for their services enough information to start skewing the results.

Mr. Matt Jeneroux: Okay. I'm done.

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

Our next seven minutes go to Mr. MacGregor.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Thank you very much, Mr. Chair.

Mr. McLinton, the committee received a letter from the commissioner, and in that letter the commissioner identified a few concerns. It was a fairly lengthy letter, and it goes over the current state of the laws today. One sentence stood out for me. He wrote:

> Technology and business models have changed so significantly since PIPEDA was drafted that many now describe the consent model, as originally conceived in the context of individual business transactions, to be no longer up to the task: 90% of Canadians are concerned that they no longer have control of their personal information.

I'd just like to have a quick response from you on the commissioner's concerns.

● (1620)

Mr. Jason McLinton: I can only speak again from a retail perspective, and say that it's not in the retailer's business interest to do anything but be clear and simple with regard to the collection of consent, in the news that they didn't treat it appropriately. From our perspective it's a model that's been working quite well.

Mr. Alistair MacGregor: You said you feel it's better that we have a trust model and no increased enforcement powers. The commissioner's gone on to say that his predecessor did ask for stronger enforcement powers under PIPEDA, and that he has made it known to the committee that he's going to be asking for order-making powers under that act. You're not in favour of the commissioner's approach?

Mr. Jason McLinton: I'm not specifically familiar with that enforcement power—

Mr. Alistair MacGregor: It's like order-making powers and the power to impose administrative monetary penalties.

Mr. Jason McLinton: Without knowing the specifics of that, I am familiar with order powers and AMPs generally. I would say that our members would not be in favour of that for the exact reasons I expressed during my testimony, that right now under the current arbitration-type model, because of the shared goals that retailers have with the Office of the Privacy Commissioner, they can be very forthcoming with the information that they provide as opposed to being in a more formal legal context where they perhaps would be given advice where they couldn't be as forthcoming. I think in the end that would probably accomplish, at least in our context, the opposite of what's intended, that you would get less done with a more legalistic approach to things as opposed to a collaborative arbitrary approach.

Mr. Alistair MacGregor: It's noted here that the information and privacy commissioners of Alberta and British Columbia, which is my home province, do have order-making powers. Have any of your members related to you their experiences under those provincial regimes? Are you familiar with them at all?

Mr. Jason McLinton: I'm not familiar enough to comment on it. I did have conversations a little bit with regard to the fact that other jurisdictions, as I mentioned in my comments, do have privacy legislation. The feedback I received was that what's currently happening is working well, in that provinces and the federal government are speaking with each other and exchanging information, and that this is something that's working well, because it's avoiding multiple reporting requirements. But in terms of order-making authorities, I didn't engage in that conversation.

Mr. Alistair MacGregor: Okay, thank you.

Ms. Bourne-Tyson, in your opening statement you made a reference—and this is in the context of the right to be forgotten—about people trying to delist previous criminal records. I don't know if I caught it. Would you mind repeating what you stated about that, about a person's criminal past and the right to try to remove any links to that?

Ms. Donna Bourne-Tyson: I'm going to pass this to my colleague Susan.

Ms. Susan Haigh (Executive Director, Canadian Association of Research Libraries): This was in the context of a specific example that we were citing, just something that arose within our context as a research library where a thesis.... It was content that was embedded in a chapter in a thesis that somebody had authored, of course; and the thesis is put up on the Internet as part of the public record, as part of the research record, if you will, on open access. The request had to do with the fact that the individual had turned his life around, and the family came forward with a request that the whole thesis be removed from public access.

Libraries make these judgments on an ongoing basis. The judgment that was made at that time was that this was legitimately researched. It was responsible content. It had been through the ethics board to start with and, of course, there was the degree granted that it was part of the public research record. The request didn't come from the rights holder, which can change things a little bit in terms of takedown. The decision was made that it would not be acceded to as a request.

What we were really trying to illustrate, though, is that there are dimensions of this issue, that it can get complicated, and that's part of the nuance we're aiming to suggest is necessary.

● (1625)

Mr. Alistair MacGregor: I'm curious, and I'll open it up to all the panellists. When someone has gone through the effort and served the appropriate amount of time after having received a criminal record and has applied for a record suspension, how does the removal of the criminal record officially—so that potential employers won't have access to that anymore—interact with someone maybe having a record of that criminal act still online somewhere? Does anyone have any information on that?

Mr. Colin McKay: This is part of the reality in Europe, which is that while you may have the completion of the sentence and you may have some level of confidentiality imposed on the record, the reporting of the record still exists, both through the media themselves and other sources.

Then, country by country, it may be a legal requirement or it may be a judgment call on whether or not there's a request, and it's followed through, to suppress the results of those still extant news reports about the crime. That's why I pointed to the civic discourse, because there really needs to be a solid dialogue.

That has happened on a nation-by-nation basis in Europe. The right to be forgotten applies across the entire union, but it still varies between jurisdictions as well.

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

Our last seven minutes goes to Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon and thanks for coming here.

The question I have is probably most pertinent to Mr. Kozak and Ms. Bourne-Tyson. I'm sure you have very strong feelings about the right to be forgotten. We've spent a lot of time on this issue, and I just want to get your feedback. Could you give me an idea of what your European counterparts think of it?

Right now in Canada, we have four different privacy regimes. When you look at the right to be forgotten in Europe, with Europe enforcing the GDPR in May 2018, we are going to have to deal with that question here to maintain our adequacy, which is also good for us in terms of our competitive business environment here and in terms of CETA.

Have you gotten any feedback? I'm more interested in what their thoughts are. Have you spoken to them or do you have any feedback on what they're thinking, on how they're reacting to this new provision?

Ms. Donna Bourne-Tyson: In terms of how our colleagues in Europe are reacting, there are discussions and studies under way under the International Federation of Library Associations and Institutions. They have done a survey, country by country, of how this unfolds.

In general, somewhere between what's happening in Europe and what happens in the United States, Canada can perhaps find a middle way where we are more effectively balancing the rights of the public good with the individual.

Ms. Susan Haigh: I think the same thing. On the question of whether privacy trumps freedom of expression rights or whether freedom of expression trumps privacy rights, the U.S. versus European model, our sense is that there might be something, a judicious “in-between”, that is worth exploring and discussing and potentially codifying.

Mr. Raj Saini: Mr. Kozak, do you have any comments?

Mr. Greg Kozak: I don't have much to add in that regard. Unfortunately, I don't know specifically what analogous associations are doing in Europe, although I can point to the fundamental differences we have in our juridical/legal systems. The EU's is mostly based on dignity, whereas our privacy is mostly coming from liberty. Theirs is more one that is non-revokable, whereas here we do have a renounceable aspect to it. So it gets to the point of adequacy between the EU and Canada. We might not always fit precisely in trying to achieve that balance, just based on our underpinning systems here.

● (1630)

Mr. Raj Saini: When we talk about balance, I'm sure you're aware of the Globe24h.com case where there was a website that contained legal records, and there was a Romanian company that indexed those records to a name and then charged money to have the name removed.

Could that be a compromise? Information is not totally forgotten; it's held in a website but the names are de-indexed. You could have the provision of having the information retained but not having it indexed. Someone would really have to look for it; it would not come up serendipitously or just by fluke. Would that be a balance?

Ms. Susan Haigh: In our statement, that is what we were saying, that there is a likelihood that there are cases where delisting would make some sense. In some of the instances that were talked about, information is up on the web illegally anyway or is inaccurate, or perhaps it doesn't have the informed consent. Perhaps it has to do with juvenile content, and so on. That's all good....

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Mr. Kozak, do you have anything to add?

Mr. Greg Kozak: I would just point back to what I stated briefly, that our focus would be mostly upon what impact this would have on the public record. In cases where the harm to reputation diminishes over time, and certainly with deceased individuals, would we want to completely destroy listings or records? De-indexing might be a solid way of achieving that middle ground, of concealing it during a period of sensitivity, with mindfulness that this information is part of the public record and might eventually come back into the public record in a more accessible format.

Mr. Raj Saini: This question is for you, Mr. McLinton. I wanted to get your thoughts on something.

I was reading an article about how when a customer walks into a retail store now, there's technology—either through Wi-Fi or through Bluetooth—whereby you can analyze exactly where they're going in the store and where they're stopping in the departments, but consent has not been given. In terms of consent being implied or explicit, do you feel that it should be implied, or do you feel that customers should know that as they're travelling through the store they're being monitored in some way?

The reason I ask is that with cellphones and other smart phones right now, you have unique identifiers in the phone, so I know there's probably going to be some de-identification of the data. You're not linking to a name, an address, or an email, but there is a unique identifier in the phone, and that data can be reidentified in the future. Is there no worry that this could happen?

Mr. Jason McLinton: I'm personally not at all familiar with that, so I'd like to look into it. In terms of every conversation I've had with the members, they believe strongly in the idea of consent and reasonable consent: that their consumers would reasonably know how their information was being used and that they had consented to it.

Again, it's not in their business interests to do something like that. If a consumer did find out about it and was very upset, for whatever reason, for whatever happened in that particular situation, that would not be in their business interests.

I'd be interested in learning more about this, because that's not been my experience in terms of all the conversations I've had with members.

Mr. Raj Saini: I can give you the article I read.

Mr. Jason McLinton: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): That's the end of our seven-minute round.

Mr. McLinton, perhaps you could consult your membership and get back to the committee in writing.

Mr. Jason McLinton: Mr. Chair, may I also provide a point of clarification on the response I gave earlier to one of Mr. Long's questions?

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

Mr. Jason McLinton: Mr. Long, I wanted to clarify that for the members that I've spoken to, the level of awareness is very high with regard to digital privacy. RCC has not taken a lot of activity.... We have some committees, and I mentioned the privacy committee that has had various levels of activity over the years. I mentioned anti-spam and some other work we've done with the chamber, which is on digital issues generally as opposed to specifically on privacy. Some of it has to do with security.

I just want to clarify that. I don't believe it's the RCC's role to be doing that. In all the conversations I've had with members to date—members of all sizes—the level of awareness is very high. Why? Again, it's in their business interests to maintain that consumer trust.

● (1635)

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

Our five-minute round begins with Mr. Kelly.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Ms. Bourne-Tyson, in your remarks, you touched on an area that interested me quite a bit and introduced a way of looking at this that perhaps we haven't heard before. You talked about the right to erasure or to be forgotten and pointed out that de-indexing something from a search engine does not hide it, or is not the same as erasure. It's about making something more difficult to find, and the determination of the researcher is a factor in truly being able to either lose or bury information.

You also talked about business failures, criminal backgrounds, and things like that, which people would not wish to have known. It occurred to me then that for things like business failures, professional misconduct, or legal action judgments, especially perhaps those dealing with family court, these public records are created and are typically not made available on the Internet. They're public, but the researcher may have to pay a nominal fee to search, say, a land title. You can't Google somebody's land title or the title to somebody's property, but you can go to a land title office and, depending on the province, pay a few dollars and get that information.

Could you elaborate? I'd like a little further discussion about the separation of public information and online information.

Ms. Donna Bourne-Tyson: Over time, there will be less of a distinction, and really, for digital citizens to have equitable access, one would hope that everything would be available online unless there is some specific reason, a privacy-based reason, for it not to be. Again, the delisting, as opposed to removal, would meet a short-term privacy need. There is technology available that would allow the delisting to terminate after a certain point in time, such as 20 years after somebody's death. We don't even need to be doing this manually. We have the technology to set something up so that eventually this information returns to the public record.

Mr. Pat Kelly: I guess it seems that most Canadians have long been comfortable with the idea that a court judgment is public information and that land title records are public information, yet I think Canadians would be very uncomfortable if they thought you could just Google that information and find it instantly. On this line between.... I mean, there are reasons why some of these types of information are simply not available at present through search engines.

I'll let you comment if you want to add, and then I'll have Mr. McKay jump in.

Ms. Donna Bourne-Tyson: Susan can maybe say more on this.

In the government's open government initiative, the philosophy is that everything is open by default.

Mr. Pat Kelly: This is private information, though. This isn't government information.

Ms. Donna Bourne-Tyson: But I think the same philosophy can apply unless there is a privacy issue.

Ms. Susan Haigh: May I add to that? I think the question of when there is a privacy issue really is the question, and it really deserves some very careful thinking through, because, as you know, the Internet does allow much more visibility. We can take it back to the print era and think about what was in the public record but was hard to find, and what was stored in archives and took great effort—or potentially payment—to find. It was not so much available.

There is now so much opportunity to put something up and have it available for a wide range of uses, so the question changes. It changes to one of, well, is there really a privacy issue that would prevent it? If there isn't, then the open flow of information would be desirable.

● (1640)

Mr. Pat Kelly: There are 30 seconds left if you'd like to weigh in, Mr. McKay.

Mr. Colin McKay: Mr. Saini brought up Globe24h. In practical terms, there are technical barriers to strip-mining information from these sites that, as you point out, are otherwise restricted from search engines, and then making that available online to be accessed through search engines. The barrier isn't really so much a process of the right to be forgotten as it is one of technical sophistication by those sites and those site managers to realize that their information is being strip-mined and placed on another site for public access. That's the first step.

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

Interestingly, CanLII, which is a public database of Canadian court decisions, is not indexed by Google, so that's a good example.

Mr. Colin McKay: Yes.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We have Mr. Ehsassi for five minutes.

Mr. Ali Ehsassi (Willowdale, Lib.): I'd like to ask Ms. Bourne-Tyson and Ms. Haigh a question, but first of all, I'd like to thank everyone for appearing before us. It's been very helpful and very informative.

Ms. Bourne-Tyson, in your opening remarks, you were talking about the concept of a “constrained approach” to the right to be forgotten. What would the parameters be? I think the example you provided was that there had to be a court order for there to be erasure. Do you think this is one of those things where only a court order could lead to privacy?

Ms. Donna Bourne-Tyson: We have speculated that to some extent, for some of the low-hanging fruit, there could be a regime where, if it's a clear case of a minor and unfortunate photographs, this would not require any sort of assessment or an order, but in any other situation where it is more complex and you are balancing the rights of the public record and freedom of expression with an individual's rights, there would have to be a judicial order.

Mr. Ali Ehsassi: I don't know what the definition of low-hanging fruit would be. For example, when it came to this specific thesis that you were mentioning, would that be considered low-hanging fruit and necessitate a judicial order?

Ms. Susan Haigh: I would tend to say not, but I think that things like pardons.... When information is mounted on the Internet in contravention of local policy, whether it's legislated or company policy or whatever, and when these things are without consent of individuals and there is something inappropriate about it, or if the information is inaccurate in some manner, I guess, that might be a clearer case than something that really is weighing in the balance and where it's unclear whether the other rights...because those other rights are broad fundamental charter rights.

When it gets difficult like that, we are simply saying that it should be a harder process and a more measured process, and it should have a more neutral assessment, because it matters. It matters for the social fabric of the country. It's not a case where.... We don't want Google making that decision, really; that doesn't seem appropriate. Because it's hard. They're not black and white. My sense is that there are some sensitive areas that are in the middle. My archival colleague probably can speak to it better than I can.

Mr. Ali Ehsassi: Thank you.

Mr. Kozak, would you like to comment on that?

Mr. Greg Kozak: I think the library community is probably better at balancing off those freedoms of expression—journalistic, literary, artistic—versus privacy, although I would point back to how, when we do look at this, it is about personal information, which is recorded information about an individual. I certainly agree that there are probably very easy cases whereby you could probably prescribe types of information that we would be able to remove without a court order, such as child pornography, as you've said, or those types of very sensitive information where it would cause maybe more than reputational distress, but mental distress or medical or some other type of harm, so it implies a harms test that could be brought in.

● (1645)

Mr. Ali Ehsassi: Thank you for that.

Now I would ask the Retail Council a follow-up question. During your testimony, you were suggesting that as the Privacy Commissioner is reviewing PIPEDA, if there were any questions surrounding consent, you would like to be part of that conversation. Given the reality that this could very well not be the case, is there anything you would like to say here before our committee regarding consent?

Mr. Jason McLinton: I'll just say that if that is not going to be the case—because I understood that they were going to publish a report later in 2017—the main point there is that we believe in not throwing out the baby with the bathwater. The notion of consent, which is really a cornerstone of the legislation, is a really good one. It has a proven track record. The point is that if there were to be conversations about how that is interpreted, we would love to be part of that, but to put anything more prescriptive or "one size fits all" into the legislation is not something that our members would be supportive of.

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

We'll go back to Mr. Kelly for five minutes.

Mr. Pat Kelly: Thank you.

I'd like to ask each witness for a quick yes-or-no answer as to whether you support or favour the creation of an order-making power for the OPC. If I may, I'll just get a quick yes or no from each of you.

Mr. Jason McLinton: No, not anything that would be prescriptive.

Mr. Colin McKay: In just one word? No.

Ms. Susan Haigh: Is this for more powers for the Office of the Privacy Commissioner?

Mr. Pat Kelly: It's for an order-making power, as opposed to an ombudsman model. On the present ombudsman model or order-making power, do you support going to an order-making power for the commissioner?

A voice: Yes.

Ms. Susan Haigh: I would say possibly.

Mr. Pat Kelly: Possibly? Okay.

Mr. Kozak.

Mr. Greg Kozak: I live within a jurisdiction where the commissioner does have it, and I think it does have some benefits, especially for clarity.

Mr. Pat Kelly: Thank you. I just thought I'd get that out of the way and collect that information. We've asked many witnesses to give us a yes or no on that.

Going back to my earlier point, to what extent, then, does ease of retrieval weigh into this? I'll maybe back up a minute and say that PIPEDA's strength, according to many witnesses who have appeared here, is that it is technology neutral, and that is why, many have said, it has been a very successful regime over time. Yet I see this real distinction now, especially when we get into legal records and these types of things, which is that there really are almost two types of information: that which is readily available online and that which is not.

Is ease of retrieval of information something new that we have to consider? Also, does PIPEDA truly need to be and to continue to be technology neutral?

Go ahead, Ms. Bourne-Tyson.

Ms. Donna Bourne-Tyson: Ease of retrieval is a moving target. Think of the history of libraries and how arduous it used to be look something up. At one time they had card catalogues, so you had to look it up and then wander through and find your book. Things are changing every decade in terms of how easy it is to retrieve information, so I don't know that we'd want to create legislation at this moment in time based just on the fact that it's easier to retrieve information now. That's going to change. Hopefully, it's going to become embedded under our skin.

Retrieving information is going to become a very seamless, painless experience, and that's the beauty of PIPEDA: it's technology neutral and isn't based on any particular point in time and technology.

Mr. Colin McKay: Rather than focusing on the ease of access, it's more about how relevant the information is to a specific individual and the sensitivity of the information. I say that, because it's relatively easy to get information about the location of thousands of people using the Queensway at rush hour to deliver traffic information; and it's relatively easy to analyze thousands of different voice patterns in order to feed a translation program that does it automatically on the fly on your device.

It's still not really relevant to an individual, as some of the tougher questions we'll be dealing with today are when you're dealing with specific pieces of information tied to an individual that may have reputational harm or benefit.

That doesn't necessarily mean that PIPEDA needs to be reformed or that consent needs to be re-examined to address that. It is a subset of the conversation, and it's one that needs to be addressed specifically in the context of an individual understanding what information is available about them and what recourse they have to have that information removed within the context of how society thinks that information should be available.

● (1650)

Ms. Susan Haigh: I think there's a point to be made about individual identification, such as whether the individual can specifically be identified, because there's a lot of good and new information available that is flowing because it can be aggregated. It's anonymous, really, because it's large-scale information that can be mined in new ways.

I think it sort of flips the question, and it's a question of protecting only when it's individually identifiable and harmful to reputation or has some other unforeseen consequence, if you will.

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

We're out of time on the five minutes for Mr. McKay, and we have five minutes for Mr. Ellis.

Mr. Neil Ellis (Bay of Quinte, Lib.): I would like to thank everybody for appearing here today. I'll start off with Colin from Google.

I think it was Mr. Long who asked you the question about children and so on, and your answer was quite good, but I want to elaborate on that. It's up to the family unit and so on, but in today's age, I look at latchkey kids and at single-parent families. I look at how busy families are and at basic skills. We're not teaching basic skills like riding bikes, swimming, and things like these, and then I hear that come out.

I know Google is a gold standard and things like that, but should there not be some investment in technology, or are you guys investing in something? I know we control alcohol and things like that, which we don't give to our children, but then all of a sudden we give them a box that can.... I don't want to say it can cause more damage, because alcohol and drugs can, but you can cause damage in seconds, whether it's by predators or whether it's by information getting out.

I just wonder, technology-wise, when we've advanced so far.... You go to some websites and they say, “click here if you're 18.” You just put in the thing and that's good enough. I don't think that's anywhere near a gold standard, and I really feel that if that's the standard we're leaving to parents, then professionals, people like you, should have some technology or some investment in that.

I'll leave that with any of you for an answer.

Mr. Colin McKay: I think there's a challenge in the sort of prescriptive legislation that the United States has. Saying 13 is the barrier to having an account with online services effectively means that you have a world in which people pretend they're older than 13. As you said, they click on the.... Or services aren't developed for people in that age group, because the burden of trying to meet that standard is so great that the investment is very large.

That's one of the reasons why it's taken us to this point to develop some of those tools to help families and individuals try to create that structured environment. You're completely right, though, in that parents alone can't see and educate their children and you can't get children to realize the risk of their behaviour online without outside help.

I'm the vice-chair of MediaSmarts, which is a digital literacy organization, and we also work with coding programs like Actua and Ladies Learning Code to try to attack this program from two different directions—making sure that children have the technical skills to understand the devices they're carrying around and the programs they're interacting with and also making sure that their parents and their community and their teachers have the civic programming to be able to have a sophisticated conversation with people who are developing as adults around their interactions online.

To your point about—and it's a word that hasn't been mentioned yet—predators, there are specific technological investments that we and other companies are making in those particularly graphic and horrific parts of online activity. We're intercepting those as quickly as possible and working with law enforcement to eliminate that portion of behaviour online, because there's a recognition that there's a very dangerous space that needs to be addressed directly and forcefully.

● (1655)

Mr. Neil Ellis: Thank you.

Going back to Jason, my background is and was sometimes retail. I appreciate being here representing large businesses, as well as small business. When you look at large businesses and whether it's a Winners or TD bank, whether it's a business that is incorporated and has a board, and whether that's traded or not, we look at diversity of boards and whether we can be populated with more women.

But I don't really hear a lot of talk about diversification with IT people. When you set up governance boards—you know, we want a banker, we want a lawyer, we want an accountant, we want a former business owner—there doesn't seem to be that stress around the corporate board that makes decisions. Unfortunately, in business some of it is driven by profit so you say, reputation, reputation. If you look at the case of Winners, I think it's a landmark case: they stored credit card numbers on the same server. I don't know if they were fined in the end, but what they did for their customers was to say, “We'll take any returns back without a receipt”.

When I go back to fines and I look at whether my credit card was breached or my information..., I have to change my credit card for safety. I have to take some time, and that time I consider valuable. I could be doing other things.

Individual fines, things like that.... There are a lot of good corporations that keep having breaches. If you have a good brand, then your reputation comes back better. You look at the case of Maple Leaf; it's a whole different case, but again they got out of that.

When I say the retail side, I've built corporate boards, and they were driven on profit, but there's a new age of reputation and branding. You say you teach best practices. How do we integrate more IT people who are making these corporate decisions? Would it be safe to say that you see boards moving that way in your organization, or is this something that is always going to be more lawyers and accountants?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We're past the five-minute mark, so very briefly.

Mr. Jason McLinton: That obviously would be individual business decisions by each member. I think that would be an interesting conversation to have.

I obviously can't speak to any individual case, but in my mind any fine would not make any difference. The reputational damage and the threat of reputational damage is far greater than any sort of threat of enforcement powers or something like that.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you.

Our final three-minute round goes to Mr. MacGregor.

Mr. Alistair MacGregor: Thank you very much, Chair.

Mr. McKay, I think I'll just spend the three minutes with you.

You said that Google provides choice, transparency, control, and security to ensure that the people who use Google services have well-rounded protection. I just want to go back in time a little bit.

In 2014, the Privacy Commissioner found that Google had violated Canadian privacy laws through targeted online advertising. I think it had been based on a person's medical condition. Google's own privacy policy states that it will not target anything based on health, race, religion, or sexual orientation.

At the time, Google refused to comment publicly, but it did state that it had been working closely with the Office of the Privacy Commissioner and had resolved this issue. The Privacy Commissioner at the time noted that, “If an organization as sophisticated as Google had difficulty ensuring compliance with its privacy policy, surely others have the same challenges.”

You just stated that you're not in favour of any order-making power. Going forward, how does Google ensure that it will always be in compliance with these laws? Is it enough that the Privacy Commissioner raises this issue publicly, or do you favour an agreement where you're working together when these instances are raised? I just want to take note of how you take these emerging issues and prevent something like this from happening again.

Mr. Colin McKay: In this particular case in the report from the commissioner, it was a multi-month engagement with the commissioner's office on what was an exceptional instance of an advertiser not following the policies we had instituted on our advertising platform. It took some digging to identify what the Canadian complainant had seen and where, and how that had expressed itself in the ads they had seen. It was a challenging experience for us, but it was also a learning experience both for us and for the privacy commissioners.

The reason I stated to Mr. Kelly that the answer was no is that every one of the examples from previous reports of major significance that have been brought up today has had an impact and has resulted in behaviour change on the part of the company. Winners came up 10 years ago, and that had a tremendous impact on TJX, the parent company, and on Winners' attitude towards privacy controls.

The Globe24h.com case was an example of the current framework evolving as it should, in that there was no reaction to the report of the Privacy Commissioner, so the Privacy Commissioner went to the Federal Court and got an order, and the website was taken down.

At the moment, there are bad apples, and there are people who don't respond in a timely manner, but for companies like ours, the opportunity to engage with the privacy commissioners and work through both the technical and the privacy policy-based nature of the complaint in a very honest and transparent way, without the possibility of an administrative order or a monetary fine being produced as a result of that frank and open discovery, is a benefit. It's a really constructive engagement, especially in a space that is fast-moving, where you can discover individual occurrences that have extreme personal impact but don't have a broader implication like the one you mentioned.

● (1700)

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

That concludes our round of questions. Does anyone have anything additional to ask?

I have one question, if that's all right, to follow up on Mr. Kelly's and Mr. MacGregor's questioning.

Mr. McKay, you just mentioned the Globe24h.com case, and you pointed out the process, but it wasn't actually the OPC that applied to the Federal Court. They were a respondent in that case.

Mr. Colin McKay: Yes.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We actually put the onus on the applicant, who was already subject to injury in a finding of the OPC in 2015. They only got in the Federal Court and got a decision rendered in early 2017. That suggests to me that maybe this is not how a process ought to play out in a timely fashion, and that there is a need, in fact, for more order-making powers.

I understand that businesses want to come to the Privacy Commissioner and consult, and we have heard that we don't want a heavy hand per se. Where the Privacy Commissioner makes findings or renders a direction to companies and the companies don't listen to that direction, shouldn't there be fining powers at that stage?

Mr. Colin McKay: I have two observations in response to that.

We are still talking about a very small number of companies that are the product of findings and aren't responding to the findings or aren't engaging in the process itself.

Second, what would the structure of the Office of the Privacy Commissioner look like after you give it powers for administrative monetary penalties? I don't think the commissioner could continue being an officer of Parliament. Does it end up being structured like the Competition Bureau or another administrative tribunal? How do you then have that ombudsperson and public information role, as well as this stricter organization with greater enforcement powers?

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

That concludes our questions for today. Thanks very much to all of our witnesses.

The meeting is adjourned.