House of Commons
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 035 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Wednesday, September 30, 2009

Chair

The Honourable Michael Chong

Standing Committee on Industry, Science and Technology

Wednesday, September 30, 2009

● (1535)

[*English*]

The Clerk of the Committee (Ms. Michelle Tittley): Honourable members of the committee, I see a quorum.

We can now proceed to the election of the chair.

I am ready to receive motions to that effect.

Mr. Masse.

Mr. Brian Masse (Windsor West, NDP): I move that Michael Chong be chair.

The Clerk: It is moved by Mr. Masse that Mr. Chong be elected chair of the committee.

Are there any further motions?

Is it the pleasure of the committee to adopt the motion?

(Motion agreed to)

The Clerk: I declare the motion carried and Mr. Chong duly elected chair of the committee.

Some hon. members: Hear, hear!

The Clerk: Before inviting Mr. Chong to take the chair, we will now proceed to the election of the vice-chairs.

I am now prepared to receive motions for the position of first vice-chair.

Mr. Lake.

Mr. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): I nominate Anthony Rota.

The Clerk: Mr. Lake moves that Mr. Rota be nominated first vice-chair of the committee.

Are there other motions?

Is it the pleasure of the committee to adopt the motion?

(Motion agreed to)

The Clerk: I declare Mr. Rota elected first vice-chair of the committee.

Some hon. members: Hear, hear!

The Clerk: I am now prepared to receive motions for the position of second vice-chair.

Mr. Lake.

Mr. Mike Lake: I nominate Mr. Bouchard.

The Clerk: Mr. Lake moves that Mr. Bouchard be elected second vice-chair of the committee.

Are there any further motions?

Is it the pleasure of the committee to adopt the motion?

[*Translation*]

(Motion agreed to)

The Clerk: I declare Mr. Bouchard elected second vice-chair of the committee.

Voices: Hear, hear!

The Clerk: You may take the chair, Mr. Chong.

[*English*]

The Chair (Hon. Michael Chong (Wellington—Halton Hills, CPC)): Thank you very much to my colleagues for their confidence in electing me to be their chair.

I'd also like to seek the unanimous consent of the committee to continue with this meeting so that we can hear the witnesses who are in front of us today.

Assuming that unanimous consent of the committee is there, I'd ask that the witnesses who are to appear in front of us come to our table and take their positions. It will take a few minutes for them to do that, so we'll suspend for a couple of minutes.

Before we do, though, Mr. Rota, go ahead.

Mr. Anthony Rota (Nipissing—Timiskaming, Lib.): I suggest there are a few housekeeping issues that we may like to take a look at. Could we do that now while they are setting up?

The Chair: Sure. We won't suspend.

Mr. Rota, go ahead.

Mr. Anthony Rota: The first one concerns the next meeting we have with officials from the departments. What we are looking at doing is having that in camera, if that's okay, because a lot of that will be confidential. I think that's fair to ask.

The Chair: Certainly.

The suggestion from Mr. Rota is that for our next meeting on Monday, when we hear from

[*Translation*]

Industry Canada officials, the meeting be held in camera.

[*English*]

Is it the wish of the committee to do that next Monday?

Some hon. members: Agreed.

The Chair: Go ahead, Mr. Rota.

Mr. Anthony Rota: There are two other issues.

The first concerns what they are bringing forward in terms of suggestions to the clauses. Could we have that ahead of time and ask them to have it to us either by Thursday afternoon or Friday morning?

The last but not least issue is we have it scheduled to meet with them on Monday, and then on Wednesday we are scheduled to do clause-by-clause. There is not a lot of room in there. Could we postpone that until the next Monday? That would give us time to prepare for it, and it would work out much better.

● (1540)

The Chair: On the first point you just made, could we ask Industry Canada to have their suggested amendments to us this Thursday—

Mr. Anthony Rota: Thursday afternoon or Friday morning. That would give us the weekend, at least—

The Chair: Before they appear in front of us on Monday.

Could you contact Industry Canada to make that request.

Second, Mr. Rota suggested that we postpone clause-by-clause from next week on Wednesday to the following Monday.

Mr. Anthony Rota: That is the Monday after the break week.

The Chair: It will be the Monday following the break week, exactly.

Mr. Anthony Rota: So when we come back, we can start from there.

The Chair: Are there any opinions on doing that?

Go ahead, Mr. Lake.

Mr. Mike Lake: Could I just make a suggestion? If we're going to do that anyway, why not postpone the Monday meeting and have the Industry Canada folks come on Wednesday, which makes more sense for us and gives them more time? Maybe if we get their recommendations on Monday, that gives them a little bit more time to put them together, right?

The Chair: Before I take any other comments on this issue, the proposal in front of us is to have Industry Canada appear in front of this committee next Wednesday, October 7, then to go clause-by-clause on this piece of legislation on Monday, October 19.

Mr. Vincent.

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): Remember that they must also forward their recommendations and any amendments to the bill before Thursday or Friday.

The Chair: That's right.

Mr. Robert Bouchard (Chicoutimi—Le Fjord, BQ): When you say next Thursday or Friday, what date would that be?

Mr. Anthony Rota: I suggest we move the deadline to Monday, since we are going to receive questions on Wednesday.

Mr. Robert Vincent: But they are scheduled to come and testify on Wednesday.

Mr. Anthony Rota: Precisely.

Mr. Robert Vincent: We would need to have the documents in hand by Thursday or Friday of this week, to be ready for the following Wednesday. There is no meeting scheduled for next Monday.

[*English*]

The Chair: Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): I have absolutely no problem with what's recommended, but I think it needs to be said that if we're dealing with this stuff in camera, the information that's provided to us is still in camera and is secret to committee members only. I'm assuming that's accurate.

The Chair: That is correct.

Mr. Mike Wallace: Thank you very much.

Mr. Mike Lake: So just to clarify the mechanism, they would submit that information through the clerk, right?

The Chair: That's right. I've asked the analyst and I'll ask the clerk to contact Industry Canada to make sure they give us the information ahead of next Wednesday's meeting, as soon as possible, preferably by the end of the week but at the latest by Monday morning. So that will give members of this committee ample opportunity to review their suggested changes and comments ahead of next Wednesday's meeting. Then we'll have an in camera meeting on those suggested changes and amendments next week, Wednesday, October 7. Then we'll have the clause-by-clause meeting on this bill on Monday, October 19.

Mr. Masse.

Mr. Brian Masse: I just have a question, Mr. Chair. Why would we have those amendments in camera? That would seem to me to be an appropriate discussion to have in public because that's the process when you go clause by clause—you're making a submission to those amendments. I would object to going in camera for that type of discussion because there's really nothing sensitive that I can see that we would not want to have the public record reflect.

The Chair: I am at your mercy. I will do what the committee wants me to do. Mr. Rota and Mr. Lake suggested going in camera for that one meeting with Industry Canada. So unless there's consensus on this committee not to do that, then that's what we'll do.

Mr. Vincent.

[*Translation*]

Mr. Robert Vincent: I am somewhat confused about all of these recommendations. We want Industry Canada officials to forward any amendments to us by Thursday or Friday, so that we can be ready for the meeting the following Wednesday. I do not see the point of hearing from Industry Canada officials in camera, since they are the ones putting these amendments forward to the committee. On Wednesday October 7, we will be hearing from these same officials during a public meeting.

● (1545)

[*English*]

The Chair: Mr. Rota, do you have any comments on this?

Mr. Anthony Rota: Mr. Lake approached me and mentioned the recommendation and I agreed at the time, thinking it would just allow for a frank and open discussion without having to worry about what slips out, and the discussion would flow a lot freer. That was my logic in agreeing with Mr. Lake.

The Chair: Okay.

Mr. Lake.

Mr. Mike Lake: How we look at this is a procedural question, I guess. When we looked at the idea of having the Industry Canada folks here ahead of the clause-by-clause meeting, the idea was really almost an extension of the clause-by-clause, which is normally held in camera. So it was an opportunity to get clarification on those amendments that we would normally be moving in camera in a clause-by-clause meeting, giving us some time to actually take them back and consider them.

The Chair: Just as a point of information or clarity for members, clause-by-clause consideration is normally done in public, not in camera.

Mr. Mike Lake: On the bill? Okay. That's fine.

The Chair: We'll have it in public then at the meeting on Wednesday next week.

Without further ado, we'll now go to the order of the day, pursuant to the order of reference of Friday, May 8, 2009, to study Bill C-27, an act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act, and the Telecommunications Act.

In front of us today we have a number of witnesses from various organizations. They include Paul Misener from Amazon.ca; Tom Copeland from the Canadian Association of Internet Providers; Chris Gray and Jason Kee from the Canadian Intellectual Property Council; Geneviève Reed and Anu Bose from Option consommateurs; and finally we have Nathalie Clark and William Randle from the Canadian Bankers Association.

Welcome to you all.

We'll begin with five minutes of opening statements from each of the organizations represented, beginning with Amazon.ca.

Mr. Paul Misener (Vice-President, Global Public Policy, Amazon.com): Thank you very much, Mr. Chairman.

Thank you for inviting me to testify at this hearing on this very important topic and on this most excellent bill.

On behalf of Amazon.ca, let me add my voice to the chorus of praise, congratulations, gratitude, and support for your work on this matter and for Bill C-27.

I could easily spend my five minutes complimenting various features of the bill, but I believe my appearance here will be more valuable to you and your committee if I may suggest two areas for improvement with modest changes.

The first area is with respect to the consequences of honest mistakes. We have long said that honest e-mail mistakes should not be punished; that problem spammers wilfully and intentionally spam; and that reputable companies should be able to e-mail their customers without fear of legal retribution for honest mistakes. The market already provides very strong disincentives. Honest mistakes also aren't the source of the real spam problem; our e-mail boxes aren't barraged with messages from companies that accidentally sent them. Again, problem spammers wilfully and intentionally spam.

This is already recognized implicitly in Bill C-27, the purpose of which is "to promote compliance with the act, not to punish". It's also somewhat more explicitly recognized in the defence sections of the bill, proposed subsections 33(1) and 54(1).

At your June 18 hearings, CRTC Chairman von Finckenstein said the question of whether someone should be fined will be answered considering whether there was a "wilful breach" of the law. To make the bill clearly state the chairman's understanding, with which I agree, I suggest that proposed subsections 20(1) and 51(1) be amended so that only those who have wilfully contravened the act are subject to fines or damages. At the very least, the bill should be clarified in the defence sections using the words of Senator Goldstein's bill, Senate Bill 202, in section 22: "A person shall not be found to be liable for a violation...or if the violation was due to inadvertence or based on an honest mistake of fact."

These simple changes, courtesy of Senator Goldstein's wise drafting, would go a long way to clarifying in Bill C-27 the consequences of honest mistakes.

The other area that could use improvement is with respect to the duration of implied consent based on purchase. In Bill C-27, implied consent based on a purchase would expire after only 18 months. We believe that in the best interests of consumers, this period is much too short. First of all—and this is not a criticism, mind you—18 months is arbitrary, as already has been acknowledged before this committee. It's not a magic number, demonstrably different from 17 or 20 months, or 36 months. But most importantly, 18 months is much too short. It is not in line with consumer expectations and customer-friendly practices. Two obvious areas are: first, the production cycles—particularly for creators, such as authors and bands—can be much longer than 18 months. Joan Thomas won the most recent Amazon.ca First Novel Award for her book *Reading by Lightning*. Shouldn't consumers who bought this book be notified of her next book, even if it takes her many years to write it?

Likewise, product life cycles—for example, cars, headphones, computers—are often much longer than 18 months. Consumers expect notifications about new works or replacement products at the appropriate time, not at 17 and a half months. So from a consumer perspective, indefinite duration of this implied consent would be best. A limited period actually could increase commercial e-mail. Sellers may rush to beat an artificial deadline, causing a barrage of e-mail at 17 and a half months.

It's also hard to believe that limited-duration implied consent would make much difference. Our in-boxes are not full based on purchases in the distant past, and for the rare exceptions, consumers may opt out or block. If we must have limited-duration implied consent based on a purchase, five to seven years would be best for consumers in order to take into account production cycles and product life cycles.

I look forward to your questions.

Thank you again, Mr. Chairman.

● (1550)

The Chair: Thank you, Mr. Misener.

We'll now hear five minutes of opening statements from the Canadian Association of Internet Providers.

Mr. Tom Copeland (Chair, Canadian Association of Internet Providers): Thank you, Mr. Chairman. I am grateful to the committee members for allowing me to address you today concerning Bill C-27.

In addition to being the chair of the Canadian Association of Internet Providers for the last nine years, I have for almost 15 years been an Internet service provider in Cobourg, Ontario. I've been involved with the problem of unsolicited commercial e-mail, or spam, since it was first recognized as having the potential to cause harm and cost organizations and individuals millions of dollars each year to combat.

In 2004 I was invited to be a member of the ministerial task force on spam. In 12 short months we developed a tool kit approach to combatting spam, and the recommendations we presented to the Minister of Industry in May 2005 have been adopted by many nations around the world.

While junk e-mail is by far the most prevalent of online ailments facing Internet users, the Electronic Commerce Protection Act also recognizes that a seemingly benign e-mail message is often the precursor of greater viruses, such as Trojan horse programs, identity theft, fraud, and other criminal activity.

CAIP has several areas of concern that I'd like to bring forward today. Most of these are focused on enforcement. We are happy that the oversight of the ECPA will rest with Industry Canada. In my opinion, there isn't another department within the Government of Canada that has the experience with electronic communications that Industry Canada has. Our first concern regarding enforcement, however, lies in the enforcement agencies named in Bill C-27. While the chosen agencies have had some influence in electronic communications in the past, the will or ability to enforce their individual mandates has at times not been effective. In some instances, they have lacked the tools, mandate, or resources needed; in other instances, they simply failed to apply the tools at their disposal.

Our primary concern in this regard is with the Canadian Radio-television and Telecommunications Commission. We realize that a new function within the CRTC is being developed to accommodate this new mandate. But given the commission's adversity to enforcement of decisions and orders under its traditional telecom mandate, we have reservations regarding the willingness of the commission to exercise its new powers under Bill C-27. Despite precedent, it is my hope that these fears will not be realized and that the CRTC will gain a new appreciation of the powers bestowed upon it.

We have fewer concerns with the role played by the Office of the Privacy Commissioner and the Competition Bureau. In fact, we're pleased that their mandates have been reinforced with additional clarity, tools, and resources through Bill C-27 and other legislation. Certainly, the privacy commissioner has shown significant leadership in combatting spam to date, and the Competition Bureau has long been the watchdog consumers could turn to regarding deceptive marketing and truth in advertising. We trust that through the focus on spam that Bill C-27 provides, the leadership will continue.

With multiple enforcement agencies, however, there can come multiple agendas. In this instance, there can be no turf wars if we want Bill C-27 to be successful. The bill quickly gained legs because parliamentarians of all stripes saw value in the effort and benefits in the outcome. Our enforcement agencies must keep this example in mind as they undertake their new duties to protect Canadians online.

CAIP would like to suggest that the three agencies consider developing a trilateral task force to implement and manage their new responsibilities, rather than attempting to work in isolation. The benefit of this approach would be a reduction in duplicative efforts, more timely and effective management of complaints, better coordination of information exchanged between agencies, better use of investigative resources, and better use of financial resources.

Our second concern over enforcement has to do with the coordination of international efforts. To be effective, coordination must go beyond these hallowed halls and beyond this country. Electronic crimes know no boundaries—their perpetrators do not respect international borders. Cyber criminals do not work nine to five in the eastern time zone—they're international in scope, plying their trade 24/7, 365 days a year. Fortunately, by many estimates there are only a few ardent spamming operations in the world. Unfortunately, they operate simultaneously in many countries in nearly every continent, using unwitting Internet users as their pawns.

Despite being one of the first nations to develop a tool-kit approach to dealing with spam, we are one of the last major economies to fully implement a spam strategy based on the recommendations of the task force. The countries that have adopted these recommendations have gained expertise and developed resources capable of benefitting Canada.

The ECPA permits Canadian enforcement agencies to exchange information with other like-minded international agencies. We'd encourage the agencies to seize this opportunity and exploit the international expertise available to them in fulfilling their mandates. Because Canada is a relatively small source of spam, it is only through open and coordinated cooperation with other like-minded international enforcement agencies that we will be able to make progress in the control of spam.

● (1555)

Our third concern over enforcement is in the delivery of an appropriate and measured response when dealing with offenders. It would be our hope that legitimate Canadian business owners who make honest mistakes in deploying their online marketing strategy don't become the target of overzealous enforcement simply because they are the low-hanging fruit and easy to identify. It's the egregious spammer and nefarious e-mailer for hire that we hope will be the target of enforcement.

Rather than accumulating quick numbers and claiming great success by pursuing SMBs, we would encourage all three enforcement agencies and Industry Canada to undertake a concerted business and consumer awareness campaign to educate Canadians about the ECPA. Education is far more effective and less expensive than the cost of enforcement.

Finally, there are several simple things to remember that we think will help in developing regulations that will successfully enable enforcement of the ECPA. One, focus on the egregious perpetrators. Two, focus on the intent of the action, not necessarily the action itself. Three, focus on well-defined activities deemed to be dangerous, while at the same time providing the ability to expand those defined activities as technology changes. Four, focus on education of e-mail marketing etiquette. Five, focus on the use of enforcement as a measured and targeted tool based on the harm caused, not the inconvenience perceived. Six, adopt the best practices in legislation, regulation, and enforcement of other jurisdictions. Seven, develop a legislative and enforcement response that protects Canadians and doesn't burden them with unnecessary red tape and confusion in pursuing justice. And finally, develop a legislative and enforcement response that doesn't create criminals or create financial burden when there was no intent to defraud or harm.

Thank you.

The Chair: Thank you very much, Mr. Copeland.

We will now hear an opening statement from the Canadian Intellectual Property Council.

Mr. Chris Gray (Director, Canadian Intellectual Property Council): Thank you, Mr. Chair.

My name is Chris Gray. I am the director of the Canadian Intellectual Property Council.

Appearing with me today is Jason Kee, a steering committee member with the CIPC. He is also the director of policy and legal affairs with the Entertainment Software Association of Canada.

It is a pleasure to be able to present the views of the Canadian Intellectual Property Council and our members on Bill C-27.

The CIPC was founded in 2008 under the authority of the Canadian Chamber of Commerce to unite businesses and press for an improved intellectual property rights regime in Canada. While our focus of late has been on the copyright consultations and seeking better border enforcement to fight counterfeit goods, we also need to monitor other legislation that could affect businesses, such as this one.

The CIPC and all in the business community support the notion of eliminating spam. As we all know, spam is a nuisance to almost everyone. For a business, especially a small business, it can slow down legitimate business practices and it takes time to delete. However, there are some concerns about Bill C-27 that need to be addressed, and we're pleased that the committee is taking the time to get it right and consider amendments to the legislation that will make it acceptable to all.

Working with the Canadian Chamber of Commerce and other business associations, we've submitted amendments to the committee members for consideration. While we support the bill's objective of deterring the most dangerous forms of spam, such as phishing and malware, that discourage reliance on electronic means of carrying out commercial activities, we can't support the bill as currently drafted.

This new Electronic Commerce Protection Act may render thousands of commonly used computer applications illegal. It would submit Canadian businesses to potential fines of up to $10 million and potential civil action. This new bill would also amend the Personal Information Protection and Electronic Documents Act to submit Canadian businesses to civil suits relating to violations of the act. This bill would potentially prohibit the formation of new business relationships over the Internet or through e-mail. It would also severely limit the use of the Internet for the distribution of software and software updates.

I'm now going to turn this over to Jason to discuss some more specific concerns we have.

● (1600)

Mr. Jason Kee (Director, Policy and Legal Affairs, Entertainment Software Associaton of Canada, Canadian Intellectual Property Council): Thank you very much, Chris. Thank you, Mr. Chair.

I would like to reiterate the CIPC's support for the objectives of the bill. The Minister of Industry has clearly signalled that strengthening Canada's digital economy is a top priority for Canada and that encouraging reliance on electronic commerce by addressing issues such as spam, phishing, and malware is an important component of it. However, the broad scope of the current bill, the absence of exceptions for many socially and commercially valuable business practices, and unwieldy consent requirements collectively capture an array of legitimate activity. When coupled with massive administrative monetary penalties and statutory damage provisions, both of which impose a tremendous level of potential liability on businesses for any breach of the bill, the bill may actually have the opposite effect, actively discouraging electronic commerce in Canada and impeding the development of our digital economy.

Over the course of the committee's study of Bill C-27, a general consensus has emerged among the business and legal community that the bill should be amended so that it properly addresses the egregious and harmful forms of spam, phishing, and malware that it's intended to target while at the same time limiting its impact upon legitimate activity. To this end, as Chris mentioned, we have submitted a series of recommended amendments to the bill for your consideration. However, in the interests of time, I'm going to focus my own remarks on two key issues, namely address harvesting and anti-malware.

In terms of address harvesting, the ECPA seeks to ban the collection or use of electronic addresses obtained through address harvesting programs, as well as the collection and use of personal information obtained by telecommunications. However, the new prohibition is so broad as to prevent the collection and use of electronic addresses and other information, such as IP addresses, for legitimate purposes such as law enforcement, which will undoubtedly have very serious consequences on the ability to fight such computer crimes as child pornography and identity theft. This would also prevent the collection and use of information for legitimate private purposes, such as collecting information online to investigate instances of defamation or of potential trademark or copyright infringement or to send messages in connection with the protection of such rights.

Consequently, the address harvesting provisions should be limited to collecting address information or personal information for the purpose of sending unsolicited commercial messages, and at a minimum, the exceptions under PIPEDA for collection and use of personal information should also apply.

Regarding anti-spyware, the provisions in the bill make it illegal for anyone to install a computer program on another's computer system without express consent. While the intent of this is to prohibit installation of such malicious software as viruses, worms, and Trojan horses on individuals' computers, the definition of "computer program" is so broad as to capture any form of data, be it text, software, code, or otherwise, that causes a computer to perform a function when executed.

Consequently, it applies to the installation of an entire operating system, to the addition of a single feature in an individual piece of software, and to everything in between, including firmware updates, patches, upgrades, add-ons, etc. It applies regardless of the circumstances under which the program is installed—either installed by a professional technician, by an end-user, or via automatic update—or how it might be delivered, either being pre-installed on the device, purchased or retailed or delivered by electronic transmission, or of whether it's malicious or beneficial.

Further, it applies to any computer system, which not only includes personal computers, but also any form of consumer electronics, such as mobile phones, digital audio and video recorders, video game consoles, even most modern appliances in automobiles. If the intention is to prohibit forms of malware that discourage the reliance on electronic means of carrying out commercial activities—

The Chair: Mr. Kee, I'm sorry to interrupt. The translators are having trouble keeping up with your rapid speech. If you would allow them to keep up, that would be great. Thanks.

● (1605)

Mr. Jason Kee: If the intention of the bill is to prohibit forms of malware that discourage reliance on electronic means of carrying out commercial activities, the sweeping prohibition goes far beyond what would be required and would have the potential of doing considerable damage to the development, sale, and distribution of commercial software in Canada, thus potentially doing more to discourage electronic commerce in Canada and the development of our digital economy than the malware it purports to target.

Lastly, all computer programmers must receive express consent from the user before a program is installed and must disclose the function, purpose, and impact of each individual computer program for that consent to be valid. Accordingly, each individual computer program that's installed must be individually identified and the function, purpose, and impact of each described prior to obtaining consent. Most software routinely installs and executes a multitude—potentially hundreds or even thousands—of small computer programs during the course of its operations in order to work. Obtaining express consent from the user, including a description of the specific function, purpose, and impact, each time a program is installed and executed would simply not be technically feasible; moreover, it has the potential of being highly disruptive to the end-user's experience and could even disrupt the operation of the software itself.

Rather than institute a general, sweeping prohibition, the anti-malware provisions of the ECPA should be expressly targeted to clear instances of malware or spyware that causes harm to the end user and should provide a specific and exclusive list of computer functions that are considered to be spyware activities, as is done in the case of many anti-spyware laws that have been passed by individual U.S. states. Alternatively, the provisions of the ECPA should be narrowed to only apply to computer programs installed on another system for malicious purposes.

I would like to thank the committee for the opportunity to speak here today. I look forward to any questions you may have and to working with you to improve this important bill.

The Chair: Thank you, Mr. Kee.

[*Translation*]

I would now like to turn the floor over to Option consommateurs.

Ms. Geneviève Reed (Head, Research and Representation Department, Option consommateurs): Mr. Chair, Mr. Vice-Chair, members of the committee, thank you for this opportunity to present out views on Bill C-27, the Electronic Commerce Protection Act.

Option consommateurs dates back to 1983. We are a non-profit association with a mission to promote and to defend the interests of consumers and to ensure respect of their interests. Our head office is in Montreal. We also have an office in Ottawa.

The Task Force on Spam submitted its report to the federal Minister of Industry more than four years ago. The Task Force consisted of the ten official members, of whom I was one, drawn from private industry, government and the non-governmental sector. About 100 others with a deep-rooted interest in the question also contributed. The Task Force submitted a unanimous report in which it recommended, among other things, the drafting of a stand-alone law that would clearly address spam, spam-related offences and emerging threats such as spyware and botnets.

We therefore welcome the tabling of Bill C-27 as a first step in improving Canadian consumer confidence in electronic commerce.

It is the recipients, namely Internet Service Providers, business and consumers, who bear the cost of massive volumes of commercial email, not the senders. And these direct costs—bandwidth, filtering technology, the hiring of extra staff—and indirect costs—loss of productivity, loss of genuine messages, corruption of information technology infrastructure and identity theft—are as numerous as they are hard to quantify.

Fraudulent use of email addresses directly undermines the public confidence necessary for electronic commerce. Spam violates two different principles of privacy protection: the collection and use of information and the Internet user's right to withhold consent to such collection. Spam is also an important vector for phishing attacks which enable Internet criminals to carry out identity theft. According to the OECD, spam levels are high enough that they are undermining user confidence in email and other electronic media as well as creating a negative impact on global communications networks.

This situation makes it urgent that Parliament adopt clear precise legislation banning the sending of unsolicited and unauthorized commercial emails—as stipulated in subsection 6.1; modification of message headers—section 7; the installation or use in an individual's computer of programs without that individual's consent—section 8; misleading and fraudulent representations—section 71; the use of computer program for searching for, and collecting, electronic addresses and the use of an individual's electronic address collected by such a program—section 78; as well as the unauthorized use of a computer for the purposes of collecting personal information—section 78. It is just as important that this legislation should allow commercial email only if the consumer has clearly agreed to receive them.

In discussion groups and in a Canada-wide survey which we conducted in 2004, Canadian consumers expressed a preference for a system requiring a consumer's explicit prior consent before any commercial email is sent. We would have preferred a strict regime of explicit consent, but we consider that the thrust of sections 10 through 13 of the bill represents a reasonable compromise between explicit and implied consent in cases of an existing business relationship. For the sake of greater clarity on the point of implied consent, we recommend the addition of the following clause after clause 10.4:

> In the case of "existing business relationships", an implied consent is valid only if the recipient provides his or her own details directly and if the goods or services being marketed are similar to those previously sold to him or her,

The bill incorporates the Task Force on Spam's recommendations, firstly, that the new offences created by the law should be covered under civil status and secondly, that there be a provision allowing individuals and businesses to lodge private actions. The high financial penalties in the proposed legislation strike us as severe enough to discourage spammers.

Bill C-27 also incorporates several amendments to the Competition Act and to the Personal Information Protection and Electronic Documents Acts which will help to counter spammers' methods and practices more effectively.

Overall, the drafting of Bill C-27 seems to have been based on the best regulatory practices of Canada's many commercial partners who have already adopted legislation against spam and its harmful consequences.

● (1610)

As you undoubtedly know, the effectiveness of any legislation depends on its enforcement. As such, additional resources must necessarily be provided along with any new statutory provisions. Furthermore, this draft legislation calls for increased coordination among existing agencies named in the bill and involves the creation of a national coordination centre to monitor and report on the law's effectiveness, to support national and international cooperation, to work with industry to analyze trends in electronic threats and to develop awareness and education programs.

Finally, there is one element which needs the attention of parliamentarians and of the Government of Canada. Canadian consumers need a simple and effective complaint mechanism.

The new legislation has made provision for establishing new monitoring and new electronic risk analysis mechanisms. These will help bolster consumer confidence in electronic commerce and will help prevent potentially even more dangerous threats from developing.

Thank you very much.

[*English*]

The Chair: Thank you very much. *Merci. Et maintenant*, the Canadian Bankers Association.

Mrs. Nathalie Clark (General Counsel and Corporate Secretary, Canadian Bankers Association): Thank you, Mr. Chair and members of the committee. Thank you for inviting us to be here with you today to contribute to your study of Bill C-27, the proposed Electronic Commerce Protection Act, ECPA.

[*Translation*]

We welcome this opportunity to comment on this important bill.

[*English*]

My name is Nathalie Clark. I am the general counsel and the corporate secretary of the Canadian Bankers Association. With me today is Bill Randle, our assistant general counsel.

In the submission we have provided to the committee, we have commented on Bill C-27 in some detail. But in these opening remarks, I will briefly review our main concerns with the bill.

In recent years, criminals abused e-mail both to deliver spyware, which can steal personal information from its targets, and to send counterfeit messages that lure individuals into disclosing personal information that results in identity theft.

[*Translation*]

It is widely recognized that these types of spam are a significant threat to individuals, businesses and the Canadian economy. For several years, the CBA has encouraged the government to introduce legislation to address the most malicious forms of spam.

Canada is the only G8 country that does not currently have specific anti-spam laws and the banking industry agrees that legislation is required to protect consumers and businesses from these dangerous and damaging forms of spam.

[*English*]

As a result, we welcome the government's decision to proceed with draft anti-spam legislation and we support the stated goal of Bill C-27 to promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities. We note, however, that Bill C-27 is clearly more extensive and restrictive than similar legislation in other jurisdictions, including the United States.

We are concerned with the broad range of the bill and the potential negative impact that some of its provisions may have on legitimate business activities. In particular, we believe the opt-in framework proposed in the bill, combined with the need—with some limited exceptions—to obtain express consent from a person to send them a commercial electronic message, will have a negative impact on the ability of legitimate businesses to market their goods and services electronically. Most importantly, express consent cannot be obtained by sending an e-mail or other electronic communications to a person requesting consent. It can only be obtained in some other manner through some prior contact with the recipient. In other words, a business cannot send an unsolicited electronic message seeking consent to send more messages.

We recommend, therefore, that Bill C-27 be amended to allow the sending of an initial contact message without consent, while strengthening the content requirements of the initial contact message to ensure it is consistent with the principles of the do-not-call list legislation and the anti-spam legislation of other countries.

We acknowledge that consent can be implied when there is an existing business relationship—we welcome this exception—but believe some changes are needed to the definition of “existing business relationship”. We also recommend an amendment to extend the exception to affiliates of a company with which a person has a business relationship.

● (1615)

[*Translation*]

We note that express consent is required every time a “computer program” is installed, even when there is an existing business relationship. We would like some clarification that tools such as “cookies” are not included in the definition of “computer program” set out in the bill.

[*English*]

There is an extensive system of administrative monetary penalties set out in the bill as well. While we accept that there is a need for an enforcement regime, including penalties for persons who breach the provisions of the act, we believe that some aspects of the regime, and especially the penalties proposed in the bill, are excessive and would discourage businesses from engaging in legitimate marketing activities. This could have the effect of stifling the development of legitimate electronic marketing and could adversely affect the ability of businesses to reach their consumers.

The bill states that the purpose of these substantial AMPs is to encourage cooperation and compliance with the legislation and is not to punish. If that is the primary objective of the AMP provision in Bill C-27, we recommend that the CRTC be given the ability to suspend an AMP for a period of time, and if the persons subject to the AMP satisfy the CRTC that they have made changes to comply fully with the law, then the AMP could be withdrawn.

The bill also includes a private right of action that allows for statutory damages without proof of loss. We believe that the appropriate enforcement regime is government based. We do not support a private right of action, as we believe that these actions are generally motivated more by private monetary considerations than by general deterrence, and that a private right of action will have a chilling effect on businesses that wish to engage in legitimate marketing activities. While the bill provides for various factors to be considered in assessing damages under a private right of action, legitimate businesses are still put to the significant cost and task of defending themselves in this context. In particular, the private right of action that allows for statutory damages without proof of loss will encourage class actions that will lead to substantive legal costs and reputational risk for businesses.

● (1620)

[*Translation*]

Summing up, the CBA stands firmly behind this legislation that protects individuals, businesses and the Canadian economy from the serious threat of malicious forms of spams. We are very pleased to have had this opportunity to work closely with the government and with members of Parliament to ensure that Canada is no longer the only G8 without specific anti-spam laws on the books.

[*English*]

Thank you once again for providing the CBA with the opportunity to offer our views on Bill C-27. We would be pleased to answer any questions.

[*Translation*]

The Chair: Thank you, Ms. Clark.

[*English*]

We'll have about an hour and 10 minutes of questions and comments from members of this committee, beginning with Mr. Rota.

Mr. Anthony Rota: Thank you, Mr. Chair.

I'd like to point out that it's my understanding that today is International Translation Day, and I know, just based on both languages going on here very quickly, that the translators have certainly earned our acknowledgement today. I just want to acknowledge the translators.

Voices: Hear, hear!

Mr. Anthony Rota: And I want to thank the witnesses for coming out today, of course.

My first question is to Mr. Misener and Mr. Gray.

One of the concerns with this bill is that it is very broad and encompasses absolutely everything. One of the concerns that has come up is that something so broad will really compromise a lot of our Canadian companies. Really, on an international basis, much of the malware or the e-mail that comes in that is unwanted is coming from outside the country. What does this do to Canadian business? Does it compromise us? Does it tie our hands behind our backs and ask us to market unfairly from outside the country? If you could comment on that, I'd appreciate it, Mr. Misener, and then Mr. Gray.

Mr. Paul Misener: Thank you, sir.

I would have to answer simply no, I don't believe it does compromise the ability of Canadian businesses to compete and do well. Amazon.ca is generally happy with the provisions here. We've articulated a few areas where there are some pro-consumer practices that are already expected by consumers that might be foreclosed by some of the provisions, but with the minor modifications I've suggested, I think Amazon.ca will have no problem competing in this environment.

We fully recognize that there are needs for international cooperation, and I think that's been roundly applauded. The idea that we would somehow want to isolate ourselves and cut ourselves off from the rest of the world is a bit naive, because so much of it does come from overseas. So there is the need for international cooperation.

When I spoke before as part of the Canadian delegation at the OECD event in Seoul last year, I mentioned this need for international cooperation. We fully support that.

Mr. Anthony Rota: That's very good. Thank you.

Mr. Gray.

Mr. Chris Gray: Thank you for the question.

I'll just say briefly that we at the CIPC do think that it would affect our ability to compete. It would be detrimental.

I'll turn it over to Jason, who will get a bit more into the specifics.

Mr. Jason Kee: To give just a quick response, we concur entirely with that notion. It raises a very valid point. It also goes to what Mr. Copeland was saying about the percentage of spam that is actually coming in from abroad as a percentage of total spam.

Clearly, everyone acknowledges the significant problems caused by the volumes of spam we see generally. But to the extent that this bill is clearly going to be applying principally in Canada and affecting Canadian spammers, and in looking at that and to what extent it is actually going to stop or stem the flow of the volumes of spam that we're seeing, vis-à-vis the kinds of costs that it can impose on Canadian companies in terms of significantly limiting their capacity to engage in essentially online commerce, this is something the committee should consider very seriously when they're doing the bill.

Mr. Anthony Rota: That's very good.

My next question will go to Ms. Clark and Mr. Randle.

The private right of action is something that concerns me. When somebody does something wrong, usually it's a government agency that presses charges or there are fines that are imposed.

On allowing individuals to seek recompense for something that they perceive has been a wrong, how can you see this happening for companies? Do you see class action suits coming out? It sounds like it could be a very lucrative business for certain legal professionals.

● (1625)

Mrs. Nathalie Clark: As I said in my opening remarks, we believe that a private right of action in this context is inappropriate. We believe there is a risk of facing increased private actions that would put a lot of pressure and costs on our industry. There's always a risk of class action when there's a civil right of action. We believe it is better for the government to deal with any breaches of the act and we believe that would be an appropriate channel to deal with the breaches.

Mr. Anthony Rota: So are you suggesting removing the ability for an individual to sue someone who sends him an e-mail or malware?

Mrs. Nathalie Clark: I guess I would answer that question by saying that what really concerns the industry is that built into that private right of action is a possibility to have damages granted without a real proof of loss. That is really the issue we have with this regime. We think it's inappropriate to be able to grant damages when no real loss has been proven. In that sense, we don't support the private right of action as it is drafted in the bill currently.

Mr. Anthony Rota: I'm just trying to think this through. I'm on my computer and I'm working on a program or, let's say, an offer to someone I'm seeking business from. A piece of malware comes in through the e-mail. I open it up and it takes over my computer and shuts it down. Under what you're suggesting, I would have no recourse in regard to the person who caused the problem in the first place.

Mrs. Nathalie Clark: Well, I think if the power is given to the regulator to monitor compliance with the act, you will have the possibility of bringing that issue to the regulator, and it will be for the regulator to enforce the act appropriately after a formal investigation.

So in that sense, I don't think it is true to say that you have no possibility of recourse. What we're saying is that the government should be dealing with any non-compliance with this legislation, and that it is appropriate that it be this way.

Do you have anything to add, Bill?

Mr. William Randle (Assistant General Counsel and Foreign Bank Secretary, Canadian Bankers Association): I would also say that our real concern was with the fact that they could pursue the right of action and the class actions on the private right of action. Put those things together in the development of class actions in this province and the costs for businesses, especially small and medium-sized businesses, can be quite significant in defending these actions.

Our focus was on that and the impact it might have, especially if there's no real need to establish a real loss. I think in the example you gave there was a potential loss, and that might be something for the committee to consider, but our concern is this sort of complete right of action simply because something happened to them that was a breach of the legislation.

Mr. Anthony Rota: It's wasted my time, and my time is precious; therefore, I can sue. That's the kind of stuff we're trying to stay away from.

Mr. William Randle: And as you say, Mr. Rota, we've all been faced with individuals who may have certain ways of dealing with things, and I think it's unfair to companies that.... In fact, as a number of the other witnesses have said, you could have an honest mistake that potentially would lead to a right of action in this bill.

The Chair: Thank you very much, Mr. Randle.

Monsieur Bouchard.

[*Translation*]

Mr. Robert Bouchard: Thank you, Mr. Chair.

I too would like to mention the fact that it is International Translation Day. I want to thank the interpreters because I rely on great deal on their services.

I would also like to thank each one of the witnesses for coming here to testify this afternoon.

My first question is for Mr. Paul Misener. You can let me know if I am giving an accurate synopsis of your presentation. You stated that there should be no restrictions or limits on business-to-business emails and that between a business and a consumer or client, the period of implied consent for contact should be five years. Could you clarify this five-year period for me? Does the clock start when the file is opened, or when the last email or communication is sent?

Have you thought about this timeframe? Would the clock start running immediately on this five-year period you are proposing, or is there a transition phase to allow for the application of the provisions?

● (1630)

[*English*]

Mr. Paul Misener: *Merci, monsieur.*

My proposal here was to recognize that, in the context of when a consumer affirmatively goes and purchases something from a seller, there be implied consent for that seller to continue to communicate with that consumer and offer that consumer new products—perhaps a sequel to the book they purchased—and that an 18-month implied consent simply is not sufficient and it does not match consumer expectations, especially given that books aren't written every 17 months, new cars don't go bad every 17 months, and so forth. There is a real consumer benefit for a much longer period. I would argue for an indefinite period, but perhaps five years would be sufficient.

I'm sorry, what was the second question?

[*Translation*]

Mr. Robert Bouchard: My second question concerns this transition. In so far as this five-year period is concerned, when exactly does the clock start running? How do you determine the point at which you start calculating?

[*English*]

Mr. Paul Misener: It's a great question, sir.

I'm not a statutory expert. I think that's probably the date at which the act would come into force. Presumably it would start these clocks, because if you recall, sellers are required to keep track of when a customer purchased something. All of a sudden there is going to be a clock associated with every customer, and the clock presumably would have to start running at the time the act comes into force, just so we could keep track of such things and not have to try to go back and determine where the clock is.

[*Translation*]

Mr. Robert Bouchard: Thank you.

My next question is directed to Ms. Clark of the Canadian Bankers Association. You mentioned the possibility of a business or retailer contacting a person in advance to obtain his or her consent, and about the possibility of contacting that person once and from that moment on, having that person's consent.

Did I understand you correctly? What would justify that course of action?

Mrs. Nathalie Clark: Yes, it is true that we would like to be able to contact a prospective customer or consumer initially to request his or consent at that time. Obviously, we are not suggesting that strict parameters be put in place to govern the initial contact, but rather that some provision be made for this contact in the legislation. That is what we are proposing. We feel that an amendment of this nature would enable us to carry out legitimate business activities, without compromising either the intent or aims of the legislation.

● (1635)

Mr. Robert Bouchard: I have a side question. Are you talking about a business communicating with existing customers, or about communicating in an effort to attract new customers?

Mrs. Nathalie Clark: I'm talking about efforts to attract new or prospective customers.

Mr. Robert Bouchard: I see. What that means is that in the case of existing customers, you are not suggesting that there need to have been an existing relationship between the business and the client for a specified period of time.

Have you given any thought to the timeframe that could be applied in the case of implied consent? Earlier, we talked about five years. Should the period of implied consent be shorter? Should there be no limit set at all?

Mrs. Nathalie Clark: We did not consider that point. I would first like to reiterate that we support this bill. However, we believe that a number of simple amendments could address some of our concerns about legitimate commercial activities. Clearly, it is important for us to be able to make that initial contact with a prospective customer.

As for our concerns about existing customers, let me just mention that we would not be allowed to refer an existing customer to another affiliate of the bank. We want to be able to do that. We also believe that we should be able to offer an existing customer of the bank the option of being referred to affiliates of the bank or to other banking services. That is our only concern with respect to existing customers.

Mr. Robert Bouchard: I would like to hear from the representative of Option consommateurs on this matter. As we can see, there is a fair amount of latitude in terms of communication opportunities. You seem to be saying that in order for a business to communicate with a consumer, prior consent of the consumer must be obtained. Is that correct?

Ms. Geneviève Reed: You are absolutely correct. That is what we recommended further to a research project carried out in 2004. We have always maintained this position. We favour the "opt-in" framework, as do most of the Canadians we surveyed at the time, that is to say we believe prior consent must be given before a request for information is sent, if only for the fact that a person's email address is personal information.

I wonder how businesses will initially contact a consumer if there is no prior existing relationship. How will they access email addresses? That is what I would like to know.

The Chair: Thank you, Mr. Bouchard and Ms. Reed.

Mr. Lake.

[*English*]

Mr. Mike Lake: Thank you, Mr. Chair.

I have a quick point in relation to Mr. Gray and Mr. Kee.

One of you mentioned some installation issues that you had, and we've heard similar concerns from other groups with the software that's on the computer needing to have things installed from time to time to allow it to run properly. I know that's something we'll be looking at with the amendments. We've identified that there may be an issue there.

Mr. Misener, in relation to your comments around clause 10 and the 18-month window, I'd make a quick clarification. The 18-month window applies only in the case of the implied consent, so the idea of this existing business relationship.... If you, through that existing business relationship, simply ask the person buying the book or whatever it might be that they're buying for express consent, then you have that consent forever.

Is that an unreasonable expectation that a company would simply ask for that express consent so they get it, and if a new book comes out four years later, they don't have to ask again because they've gotten the express consent at the time of the original purchase?

Mr. Paul Misener: Thank you, Mr. Lake.

It's potentially reasonable, but here we've already recognized that there is a consumer expectation arising out of a purchase. This is a transaction. This isn't simply a matter of visiting a website or just receiving an e-mail; this is someone going and actually making a purchase. There is an expectation now that consumers would want to maintain some sort of relationship. It could be argued that this ought to be entirely an opt-in bill, but it's not, and it should not be. I think consumers would expect that they wouldn't have to go through the friction of providing express consent at their first purchase. Otherwise, this implied consent section wouldn't be here in the first place.

All I'm suggesting is that if we're going to have an implied consent regime, which I think is entirely reasonable and matches consumer expectations, it ought to match their expectations on the back end as well, which is to suggest that at 17 and a half months, there's not a barrage of e-mails coming in by sellers trying to maintain their buyers, but rather that it more appropriately matches product cycles and product life cycles.

● (1640)

Mr. Mike Lake: Right. And I understand the concern.

As a consumer myself, I just think that when I do purchase something, whether it be online or not, I actually don't expect that I will receive e-mails from the company that I purchased from for the rest of my life because I've made that one purchase. I think it wouldn't be that difficult for someone to actually ask me for my express consent at that time. Then if I do want to do it, I would simply put a check mark on the box, and then expect to receive the e-mails. That's just a point from personal use.

For Ms. Clark, I just want to clarify something. First of all, you pointed to the American legislation, in terms of an example, and said that it is different from other legislation in terms of the way it deals with things, and that it deals with some things harder than other legislation.

Now, David Fewer, who was here last meeting from the Canadian Internet Policy and Public Interest Clinic, said—and I'll quote him—that "this bill is a significant improvement over the U.S. legislation, the CAN-SPAM legislation", which, frankly, he referred to as the "do not hesitate to spam bill".

Voices: Oh, oh!

Mr. Mike Lake: He said that if we were to move in that direction, we'd be going in the wrong direction.

Do you agree with Mr. Fewer that the American legislation doesn't go far enough, that we need to learn from other pieces of legislation that have been passed, and maybe mistakes that have been made, in terms of our drafting of this legislation?

Mrs. Nathalie Clark: I will let my colleague answer this question.

Mr. William Randle: Thank you, Mr. Lake.

As we said, I think we are strongly supportive of the bill generally. I think our reference to other legislation was really in relation to specific provisions in this bill rather than generally. I would agree that the civil servants and the department have obviously spent a great deal of time considering legislation elsewhere to come up with a comprehensive bill that I think there is a lot of support for. So our reference to other legislation, especially U.S., was in relation to specific provisions rather than the bill generally. I think some of the other witnesses would indicate, similarly, that while this bill is to be admired in many ways, it doesn't mean to say there aren't amendments that could make it even better.

Mr. Mike Lake: Their suggestion is to clarify, though. Is the suggestion you're making that any company could send out an e-mail to me without having any relationship with me whatsoever, to ask me if I want to have a business relationship with them?

Mr. William Randle: Are you discussing the initial contact message?

Mr. Mike Lake: Yes. Is that your proposal, the initial contact message?

Mr. William Randle: Our proposal is that in this day and age, where more and more companies are dealing in electronic means, and in fact that's being encouraged because it obviously lowers costs both to the companies concerned and the consumer, we should try to have a balance between the need to avoid malicious spam and allowing companies to continue to have legitimate business activities electronically. We think allowing an initial contact message to prospective customers, with suitable safeguards, as we've indicated, which would be consistent with the intent and principles in the bill, would effect that balance that we're discussing.

Mr. Mike Lake: So, hypothetically, if my e-mail address wound up on a list of e-mail addresses that was being sold, if that was the way that companies could prospect, my name could be sold to 100,000 companies, all of whom would have licence to send me one e-mail to see if I would want to give them explicit consent to buy their product.

● (1645)

Mr. William Randle: Well, that's an interesting thought, although I don't think many people would get 100,000 e-mails, to be frank. You can always take hypotheticals to an extreme, but I think in the practical sense what really happens is that a very selective number of businesses are involved in this type of business, especially if the idea was that the initial contact would have a number of restrictions on it as to how it would be sent.

With respect, I don't think you would end up with 100,000 companies going to the time and trouble needed to prepare this type of initial message.

Mr. Mike Lake: But the fact that you're proposing it would indicate that you would defend that as good, strategic policy for a company, to get e-mail addresses and then send that one e-mail out, right? So would it not stand to reason that any company that wants to promote itself using sound, strategic policy would actually undertake that strategy and thus send out an e-mail, and there would be tens of thousands or hundreds of thousands of businesses that might actually undertake that strategy?

Mr. William Randle: Again, with respect, I don't think there would be tens or hundreds of thousands. I think given the restrictions we suggest be placed on it, what you would find is that it would only be a small number of businesses, and a lot of them would be smaller businesses who do not have the means or resources or staff to contact prospective customers.

The Chair: Just a brief question.

Mr. Mike Lake: Actually, could I get Ms. Reed to comment on that? I would be curious to hear her thoughts.

[*Translation*]

The Chair: Ms. Reed.

Ms. Geneviève Reed: Thank you.

Again, I have a question for any business seeking to make that initial contact. How will obtain the email address of the person it wants to contact? That is all I want to know.

The Chair: Thank you, Ms. Reed.

[*English*]

Thank you, Mr. Lake.

Mr. Masse.

Mr. Brian Masse: Thank you, Mr. Chair.

My first question is for Mr. Misener. Your definition of a consumer is basically someone engaged in purchasing from somebody else. Now the unfortunate thing with that is it could apply to just about anything anywhere, because we're a consuming society. It would apply to everything from food to stores, shops, and so forth. Your business happens to be a very successful one in terms of marketing and using the Internet, especially in the early days and with the convergence of media and the products you sell.

I looked at your request to change the 18-month period of implied consent, and I guess the question I would have is, yes, I could have bought a book and enjoyed it, but I could also have bought a book and not liked it. So why should you have that right to have the next one, as it were, come my way?

Voices: Oh, oh!

Mr. Paul Misener: That's a good point—but the next one could be better!

There are many ways for feedback on particular products to be registered at Amazon.ca. Certainly our customers are vociferous in their recommendations, both pro and con. So it's very helpful to consumers who shop on the site.

I'm just saying that if you're going to have an implied consent based on a purchase, 18 months just doesn't make sense. It has to be a much longer period for that to be meaningful to consumers. I've thought not only about similar products but also of replacement products, things like electric shavers or headphones with limited lives. You don't want to get an e-mail about the possibility of replacing that product within 17 and a half months, because it better still be working by then, but after four years, that would be a useful offer to receive.

Mr. Brian Masse: Well, it might be an incentive for businesses actually to have the warranty time be the time they can contact you back. From a consumer perspective, I would argue that.

Now if I could move to Mrs. Clark and Mr. Randle, I think there's been a point missed in all of this. For example, I buy my own computer, I pay for the Internet service, and I go to my bank online and end up paying a service fee for that, and then I face a pop-up window with a survey question I have to answer before I can even get into my own bank account.

Isn't it really a privilege to be able to send me an e-mail on a service that I'm paying for, on equipment I've bought, through a medium I control, and on business transactions I am paying a premium for with an institution to begin with? Shouldn't it be the other way around? Isn't it really just a privilege that you can actually send somebody some information about a new product or service?

● (1650)

Mrs. Nathalie Clark: I think your question is in relation to online banking.

Mr. Brian Masse: No, even in general. I think there's been a lack of recognition that consumers are the ones who are paying for this infrastructure through taxes—and, actually, many times through subsidies from government programs to create the Internet at the speed and duration it works right now. There's more money that's going to be added to that. Then personally, as a consumer, you are paying for the entire infrastructure or the operating costs, and you're giving a portal or entry into that in which you've invested.

Mrs. Nathalie Clark: Online banking is done at a bank website that customers such as you access proactively to take care of their personal finances. These online banking portals were developed to respond to a customer need, to customers who wanted to use electronic means to do their personal finances.

Now it is also a means for financial institutions to get into contact with their customers, because very often that customer will not go into the branch or call the bank. So it is also a way to have a dialogue with the customer.

I think you made reference to an opportunity the bank has to send messages to their customers. Some of our online banking websites have these windows where they send you information. Very often they will do so identifying a need. Sometimes they will use these types of messages to respond to specific questions, depending on what's available on the website.

But it is a proactive step taken by the customer to enter the website, and for the bank to respond to a customer need. Therefore—

Mr. Brian Masse: Quite frankly, some of that need is because so many banks in my riding have closed, so that your options are much more limited. It's been a changing environment that has also led to some of the need out there.

My problem, really, is that I consider it to be spam that I have to answer a question of a survey on my behaviour, which goes into another file somewhere else, to get into my own account. I find that offensive, because I'm paying for that account. I think Canadians deserve a lot more credit. They can surf your Internet site and find out what's available to them and decide when and how they need to use it. I think we've turned this upside down.

Do I have time for one last quick question? Thank you, Mr. Chair.

I do want to send this out generally to everybody here, because I think it is important as an updating part of the software. I have PlayStation 3. I grew up in the gaming age. They send me a message to update my computer or my game, and I have to accept, then move through a statement and accept that statement, and then the download automatically happens. My understanding is that this process is what's being requested for other things. Maybe this would actually wake up Microsoft to release a product that's actually finished on the market. I would like to hear if that is not a reasonable way to approach update of software, of your information. I'll turn it over to the table here.

[*Translation*]

Ms. Geneviève Reed: I feel that this would be a rather sensible way of maintaining this business relationship. If I can reassure Mr. Misener at all, I would say that when that initial email is sent out, it is a simple matter of asking the consumer to tick off a box if he or she wishes to receive additional emails. Then the relationship can continue indefinitely. There is sufficient latitude in this bill to enable businesses to conduct their affairs.

[*English*]

Mr. Brian Masse: Would anybody else care to comment?

Mr. Jason Kee: I'll respond, because the Entertainment Software Association of Canada is actually the trade group for the Video Game Association.

We appreciate your support, Mr. Masse.

● (1655)

Mr. Brian Masse: I've got a PSP too.

Mr. Jason Kee: To your point—and actually, this is the core of our concern on this—what the bill is currently proposing just goes far beyond that. It requires not only that you have to obtain some form of consent, which as you mentioned is not of itself unreasonable, but it actually forces you to describe the function purpose of impact of every single computer program that's being installed during that process and to clearly identify.... To the extent that you actually may find the process of doing the update inconvenient now, can you imagine if you had literally hundreds of pages of updating for every single individual update that's happening and what the impact of that is going to be on the system?

Also, there is the corresponding issue that some of those updates are to identify security flaws that have emerged. Essentially, it would be Sony identifying to the world, “Oh, incidentally, we've identified a security flaw that lets you update the PlayStation network for free, and you can download as many games as you want. We're going to fix that. Do you agree?”

Some consumers may be—

Mr. Brian Masse: I don't mind doing it, but I get your point. It can't be so minuscule an adjustment. But at the same time, how do we balance it out? That will be the real challenge—I think we'll hear that from the department.

Mr. Jason Kee: I agree.

The Chair: Thank you very much, Mr. Masse and Mr. Kee.

Madame Coady.

Ms. Siobhan Coady (St. John's South—Mount Pearl, Lib.): Thank you very much.

Thank you to all the witnesses for being here today and for taking the time to review this piece of legislation and to give us some detailed suggestions on how we can improve it.

I'd like to ask Mr. Copeland a couple of questions, if I may, around enforcement, because you spent most of your presentation talking about that, and we haven't really delved too much into that.

I'm intrigued by your trilateral suggestion. Could you please expand upon that, as to what your suggestion would be? If you look at some of the enforcement, especially for civil liabilities and the offences thereunder, CRTC is involved and the courts are involved. Can you talk a little bit about your view on what I think you called the "trilateral task force" to manage this?

Mr. Tom Copeland: My thinking there is that it's very practical in nature. If we have three agencies trying to enforce the same piece of legislation—albeit with different responsibilities within the legislation—we're bound to have overlap at times. I think one of the overlaps that could occur is that, if I recall correctly, the Privacy Commissioner will have the ability to decline an investigation, which means the complaint would have to be shuffled off somewhere else to be re-initiated if that were the case or if new information came to light that would change the investigation. This hopscotch through the enforcement process would seem to be a little over-the-top. It would be a burden for individuals to work through, not knowing where they should start with a complaint and how it should be followed through. If there was a central cache of expertise that could be drawn upon, it would—

Ms. Siobhan Coady: Instead of trying to simplify what we're trying to do, or put more things in regulations, is there another way around this? Have you considered another way besides the suggestion of the trilateral?

Mr. Tom Copeland: I guess I am purely looking at it from the consumer's standpoint: Where do I start? To whom do I complain? Is it the CRTC? Is it the Privacy Commissioner? Is it the Competition Bureau? There is a forged header, they're trying to sell me bogus drugs, they have sent it en masse, there is no implied consent—where do I start?

To have to play that checkers game to get something started, I think, would be a deterrent to many people.

Ms. Siobhan Coady: Do you want to comment on the private right to action? We have discussed it earlier today.

Mr. Tom Copeland: Certainly, I can see the CBA's concern on that. In other jurisdictions, particularly in the United States where we have seen the private right of action used, it tends to be used when a large telecommunications provider wants to make a splash. They want to make an example of an egregious spammer. They want to seize their mansions, their boats, their cars, and raffle them off to their users for headlines.

I would hope we aren't going to see frivolous suits brought. Certainly, a lack of damages might be a concern, where with a large telecommunications provider it would be easier to identify damages because they have to deal with this stuff coming through their system. You could say each spam message is worth *x* cents, so you could compile some costs. So I think the cost of damages is important.

Ms. Siobhan Coady: Thank you.

Moving to having consent now—this is in case we haven't had consent and we're in a serious situation—I'd like to question Mr. Misener and Mr. Gray specifically around these consent provisions. There are a number of people who think the consent provisions are too narrow and are out of the context of the international community. If you look, for example, at the New Zealand spam act, probably both implied and express consent are interpreted a little differently. If we consider what has been adopted by PIPEDA and quoted from the spam task force, it defines implied consent much more broadly than this proposed act. The consent is "...where consent may be reasonably inferred from the action or inaction of the individual."

Do you think the consent provisions in this proposed act are too narrow? I think you have asked for some changes in length of time, but have you reviewed the consent provisions?

Then, Mr. Gray, could you add a comment to that?

● (1700)

Mr. Paul Misener: Thank you, Madam.

We're quite comfortable with the underlying existing business relationship. Again, this is a case of where a consumer has come and bought a product at a website, like ours or of another commercial seller, so that kind of basis for implied consent we are very comfortable with. It is simply the duration of it. If you're going to have implied consent, it ought not to expire so quickly.

The Chair: Mr. Gray.

Mr. Chris Gray: Mr. Chair, I'll simply add a brief comment and then Jason can take over.

It is definitely too narrow, as currently drafted, and needs to be addressed.

The Chair: Briefly, Mr. Kee.

Mr. Jason Kee: Essentially, one of the challenges we find with the existing implied consent regime is that it is defined by these narrow notions of the existing business relationship, existing non-business relationship. And as much as having a bright line test, where you clearly know if you're onside or offside, gives us certainty, it doesn't address the myriad of contexts in which consent can be reasonably inferred from the circumstances. Here's an example that was raised at the last meeting: someone's Facebook page. It's reasonable to infer that you would actually expect to receive messages that they're sending out—such as for campaign donations; you don't have express consent to do that, and implied consent, as drafted in the current bill, wouldn't cover that.

The Chair: Thank you very much.

Mr. Wallace.

Mr. Mike Wallace: Thank you, Mr. Chair.

I want to welcome everyone this afternoon. I appreciate your comments. We're coming down to the end of the review with witnesses and will be getting to the nitty-gritty in the next couple of weeks.

Mr. Copeland, I want to clarify, to make sure. There was a minister's task force on it. You were part of that task force, is that right?

Mr. Tom Copeland: Right. I was one of the 10 members.

Mr. Mike Wallace: I am assuming two things, but let me start with the first question. I was involved with a PIPEDA review and a number of other things. Some legislation has a timeframe to it in terms of an automatic review. Was there discussion at the task force that since this is new legislation, maybe we should put a five-year timeframe for review of this legislation and what its actual effect is? Was that discussed? How would you personally feel about it—obviously not representing the task force—if we added a timeframe to this proposed legislation in terms of an automatic review?

Mr. Tom Copeland: My recollection, and this is going back a number of years now, is that we didn't discuss a review down the road. However, technology changes. It's dynamic in nature, and certainly we can't expect that, for instance, today's definitions of an illegal cyber activity not be changed down the road. I think it would be worthwhile at some point in the future and not too far out—two to five years—to have two years for an interim review and maybe five years for a more sweeping review.

Mr. Mike Wallace: The issues the Canadian Intellectual Property Council brought forward today, or something very similar to those, I assume were discussed at the task force in terms of the scope of the bill. Would that be correct?

Mr. Tom Copeland: To some extent, yes.

Mr. Mike Wallace: I'm going to take a minute to ask the Canadian Bankers Association—I appreciate their coming—about the personal right of action. For my personal clarification, and I'll give you a banking example, I get phished, and it's happened often, I'll be frank. I'm a TD Bank customer, so I get this e-mail that looks exactly as if the TD Bank sent it. It has their logo, it's got green...and somebody's trying to get into my account. They ask for my PIN number, or whatever the number is called, so they can check on that for me. Well, they're lying, obviously. It's not from the bank; it's somebody else trying to get that information from me.

Let's say I make a mistake and give them that information and they empty my bank account. Do I not have the right to sue those folks?

● (1705)

Mrs. Nathalie Clark: I can tell you that in the past, banks consistently indemnified their clients who have suffered losses as a result of identity theft, and it's been the practice.

Mr. Mike Wallace: So your solution is that the bank will cover me and put my money back in my bank account and I should be satisfied with that.

Mrs. Nathalie Clark: Yes, that's always been the practice.

Mr. Mike Wallace: Okay.

Another question I have for you is this. Unfortunately, or fortunately, I'm on both this committee and the finance committee, and of course we review the Bank Act, which we did a few years ago. The banks are not allowed to use information they have in their branches to sell me insurance they may be providing. Not all banks provide insurance products, but some do. If my e-mail address is online for my bank, provided for mortgage purposes and other purposes, is it the bank's right to use that to send me information about insurance products they would like to sell me? Does the Bankers Association have a position on that?

Mr. William Randle: All I can say, Mr. Wallace, is that, as I'm sure you would appreciate, all our member banks follow exactly what they're required to do under the Bank Act and the regulations, including the insurance regulations.

Mr. Mike Wallace: That's not really an answer.

Voices: Oh, oh!

Mr. Mike Wallace: It's a good answer, but it's not the answer—

Mr. William Randle: I'm pleased it's a good answer.

Voices: Oh, oh!

Mr. Mike Wallace: We're starting to have an interesting discussion about whether the banks can use the Internet to sell insurance when they're not allowed to sell it through the branches. I'm concerned about their using the personal information they have from me to sell me insurance—or we change the law, one of the two.

We've heard the issue about the 18 months before, Mr. Misener, and it's consistent with the do-not-call list legislation we have here in Canada. That's my understanding, that it's consistent. One thing you didn't comment on, and maybe you can or can't, but there has been some suggestion that if you want to get off a list, you inform the supplier, and they have 10 days to take you off the list in this legislation. Some people have come to say this is too quick, and it should be 31 days. Does your organization have any issue with it staying at 10 days?

Mr. Paul Misener: Thirty-one would certainly give us more confidence, but I think we can live with 10. There are unsubscribing mechanisms in every e-mail we send to our customers, as well as on the website. You can choose to opt out of receiving any e-mail whatsoever, including legal notices. Different mechanisms are available for our customers to opt out of receiving e-mails, as well as to opt in to receiving e-mails. There are a number of services that we provide our customers whereby they can specify the kinds of e-mail they would like to receive from us. We believe this is the best balance for our customers.

Mr. Mike Wallace: Thank you.

The Chair: Thank you very much, Mr. Wallace.

Thank you, Mr. Misener.

Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent: Thank you, Mr. Chair.

Welcome. I have a question for Ms. Clark.

Earlier, you said something that surprised me somewhat. You talked about sharing email address lists with other bank affiliates. As Mr. Wallace pointed out, these addresses are personal information. We were talking about mortgages in this case.

What reason would you have for wanting to convey personal information of this nature to other bank affiliates? Who might these affiliates be and why would it be important for you to pass along personal information to parties other than the ones to whom that information was initially entrusted?

Mrs. Nathalie Clark: We are recommending that the bill be amended to allow the bank, which has an existing business relationship with its customer, to share information with some of its affiliates, in order to take a more holistic approach, so to speak, with customers. Quite often, the bank's goal is to provide the best possible service to its customers, and consequently, to provide more comprehensive services or financial advice. Our goal is to give a bank the opportunity to offer services to its customers when a need has been identified. To our minds, this is a totally legitimate business practice.

As for the other affiliates with which the bank might share this information, we can think of investment opportunities and advice offered by certain financial planners to enhance a consumer's position. Obviously, we always have the interests of our customers at heart and our goal is to provide comprehensive service so that they are aware of their personal financial situation and enjoy the best possible relationship with the bank and its financial services.

● (1710)

Mr. Robert Vincent: For example, if I do business with you, it doesn't mean that I need a financial adviser who is going to try and sell me an RRSP or some such thing. If I have a business relationship with you, there is a specific reason for it and it is not because I want to have five or ten business relationships with affiliates of the bank that want to sell me their products. Among other things, that is one of the reasons why we want to minimize this possibility. I think that is how Option consommateurs views the situation.

I agree with you that legitimate marketing activities should be allowed in order to maintain a relationship with the customer. It is not a matter of breaking off all ties with him or her. If I have a direct relationship with you and I consent to maintaining that relationship, then there is no problem. As Mr. Gray and Mr. Kee were saying, it is important to continue doing business with the customer. These days, electronic commerce is, in my opinion, the easiest way of doing that. If we impose restrictions at this time, some foreign companies will not stop their electronic commerce activities, all the more so since the door will be wide open to them.

Mr. Gray or Mr. Kee, would either one of you care to comment?

[*English*]

Mr. Jason Kee: Could you ask the question again? Sorry, I missed part of it.

[*Translation*]

Mr. Robert Vincent: We discussed business relationships with consumers, legitimate marketing practices and the fact the foreigners could continue their commerce and that the bill would restrict electronic commerce opportunities for Quebeckers and Canadians. I'd like to hear your take on the situation.

[*English*]

Mr. Jason Kee: I believe it could have a negative effect. The thrust of the point I was trying to make earlier is with respect to determining to what extent the problematic spam and other issues are emerging from Canada vis-à-vis the rest of the world and to what extent we can take effective measures to address those kinds of issues vis-à-vis the kind of cost we're imposing.

As a consequence, it's entirely feasible that at least operations that are well outside of Canada's jurisdiction, like some egregious spammer who may be located in Russia, for example, may be outside or at least beyond the scope of what we can effectively do to address the issue.

[*Translation*]

The Chair: Thank you, Mr. Vincent.

[*English*]

Thank you, Mr. Kee.

Mr. Warkentin.

Mr. Chris Warkentin (Peace River, CPC): Thank you very much, Mr. Chair.

I thank all of you for coming in this afternoon. We appreciate your testimony. We continue to try to build a piece of legislation that will effectively work for consumers but not cut out business. We thank you for your different contributions.

I want to bring it back to the discussion about the length of time we would include implied consent. Mr. Misener, you talked about the arbitrary sense of 18 months. You give an option of five to seven years. You haven't explained why five to seven years. I was wondering if that was related to your assessment of your own industry in terms of what length of time somebody would come back for a second transaction. I'm wondering if you know that specific statistic of your company as to what length of time it usually is between the time in which a person makes an initial contact and when they'll come back to make a second purchase.

● (1715)

Mr. Paul Misener: Thank you for the question, sir.

My suggestion of it being somewhere around the order of five to seven years was based on the producer cycles and the product life cycles. As producers, we sell the works of Canadian authors, and we promote Canadian bands on our website. We would want those bands to have their new releases available to people who have already purchased earlier releases and are known to them without coming back to the website.

Mr. Chris Warkentin: I'm very curious about this point. I would like to get a consumer's perspective on the whole issue of implied consent as well. Do you find that people often come back just for the same artist the second time?

Mr. Paul Misener: Absolutely, people buy within fairly narrow categories. They show they like a particular author. If, say, they bought three or four books by a particular author that they've just discovered who's written over the past decade and a half, and that author releases another work in 24 months or 19 months, we would not, under the current draft, be able to e-mail that consumer about the new release. But if they came out in 17 months since the last purchase, we'd be able to do it. That's why it's so arbitrary.

The producer cycles for an author can easily be four or five years. The product life cycle for things like computers, headphones, and such things that we also sell at Amazon.ca are not 18 months; they're more like 24, 36, or 48 months.

Mr. Chris Warkentin: I appreciate that it's going to be different for many different industries. Realtors are going to tell us that they need 20 years because the chance of somebody buying a house may be 20 years.

I'm wondering, Ms. Reed or Ms. Bose, if you've taken any time to consider the issue of implied consent and what length of time you feel the consumer would be willing to accept. Have you had those discussions with broad groups of consumers?

[*Translation*]

Ms. Geneviève Reed: Thank you.

Let me reiterate what I said earlier, namely that there is nothing to stop Mr. Misener or anyone else from sending an email to his customer during the first 18 months of their relationship to see if he or she is interested in hearing from him in future. There is absolutely nothing stopping him from doing that. It is quite easy. We receive messages like that on a regular basis. As a consumer representative, I do not have a problem with that. Whether it is in connection with a purchase or a warranty, businesses can request a customer's email address. We already see that happening. We purchase all kinds of products, credit cards and the like, and when we do, we are asked if we want to receive messages in the future. I don't see why it would be any different within the framework of this bill or how costs would be a problem.

[*English*]

Mr. Chris Warkentin: You describe the 18-month renewal of implied consent. What if it worked in reverse? If there was a pre-existing business relationship, consumers could click and say they didn't want to receive information any more. It might come two years afterwards, but when the communication came, the consumer would simply say, “Okay, no more. I'm done considering your offers.” I'm wondering if the consumer, from your perspective, would favour one over the other.

● (1720)

[*Translation*]

Ms. Geneviève Reed: Generally, speaking, consumers prefer to be asked if they want to “opt in“, rather than to have to “opt out“. That is the approach we favour.

[*English*]

The Chair: Thank you, Mr. Warkentin and Madame Reed.

Mr. Masse.

Mr. Brian Masse: Thank you, Mr. Chair.

Mr. Misener, in your letter you've encouraged the inclusion of language that would reverse the statutory punishment for an action such as using falsified headers. Maybe you could expand on this. As to the issue of a pattern of mistakes, you seem to think that if a mistake was made there would be absolute prosecution. Could you expand on that? We haven't gone very far into it.

Mr. Paul Misener: This act would prohibit some actions that are clearly intentional. No one accidentally falsifies a header, right? So if we receive e-mails from a source that looks just like RBC, that wasn't an accident—it was fully intentional. We think that in such cases it wouldn't make sense to force the prosecution or the plaintiff to show intent. Other actions could be honest mistakes. If you accidentally send an e-mail to a consumer who has asked you to stop sending more e-mails, there are serious market forces working against that kind of mistake—you don't want to annoy your potential customers. This is why we've suggested Senator Goldstein's language, which makes it clear that this would not apply if the contravention were due to an honest mistake. That kind of clarification would go a long way towards assuaging those concerns.

Mr. Brian Masse: I want to make sure I've got this right. You're saying that in the header containing false or misleading information there's more intent to mislead than if we accidentally mail something to somebody. You're worried that this might result in an upside-down situation in respect of where the fines would go.

Mr. Paul Misener: Yes, sir. The suggestions that I humbly offer would go a long way towards fixing this situation. The honest mistake would not be punished. Punishment would apply only to actions wilfully undertaken.

Mr. Brian Masse: Does anybody else have a comment on that situation?

I don't want it to seem like we're picking on the banks, but you have nine pages of issues. We had the Desjardins Bank in front of us the other day. Are they part of your association?

Mrs. Nathalie Clark: No, they're regulated by provincial legislation.

Mr. Brian Masse: You have suggested 31 days for unsubscription. I have a hard time believing it could take 31 days, especially from banks. For the most part, they are sophisticated organizations with strong communication websites. Tell me why it takes 31 days to unsubscribe. When I subscribe, I get something back within 24 hours. Being a CIBC credit card holder, I can tell you it doesn't take them long to get back to me.

Mrs. Nathalie Clark: As you said, the banks have very sophisticated systems in place. That's why we are concerned that the 10 days would not allow the banks to proceed efficiently with the unsubscription. We feel that a bit more time would help to avoid errors, delays, and non-compliance.

Banks have some of the most sophisticated IT systems in this country. At the same time, when a change needs to be done, the banks want to make sure that it is done properly, with a minimum of errors. A complex system requires more time to adjust. It might take more than 10 days to do everything properly.

Mr. Brian Masse: But if I went into my bank and wanted to be taken off the mailing list, I would expect that within a couple of weeks they could easily do that through regular, ordinary mail. I just find it hard to accept that, if the programs are that sophisticated, it wouldn't be easier—some of this is automated now—to take you off that subscription list.

It worries me that you have a system in place such that 31 days would be required. Maybe 10 business days might be more reasonable, but 31 days? That's a month.

And I don't know if that's 31 regular days or 31 business days. Can we clarify that?

● (1725)

Mrs. Nathalie Clark: It's regular days.

Mr. Brian Masse: Okay. So it's a full month.

Is there anything technically preventing the banks from being able to take people off in 10 days? Or is it just a matter of your not wanting to put in the resources to actually have either the program to do it or to have somebody do it through staffing?

Mrs. Nathalie Clark: No. Again, the only reason why we provided comment on that specific item....

I don't want to overkill it, if you will, because the banks will comply with whatever will be the intention of the legislator. The comment is really in relation to the complexity of the system. Sometimes it takes longer than you would expect to make the change and to make it right, avoiding as much as possible any errors.

The Chair: Thank you very much, Mr. Masse.

Mr. Lake.

Mr. Mike Lake: Thank you, Mr. Chair.

Since this probably will be my last time to speak to witnesses who've come before the committee on this legislation, I do want to take the time to thank you; and not just you, but also, given the subject matter, all the people following this online.

I do want to thank all of the witnesses who have been before us over the time we've been studying this bill, because it is extremely important that we get this right. I know we've heard some suggestions through our hearings that we'll definitely be considering as amendments when we move forward here. So thank you for that.

In terms of some of the conversation today, I think it's important that we remember that as we talk about consumers and businesses in this context, it's not an oppositional discussion. In fact, many of the consumers, maybe even most of the consumers we're talking about in this context, are businesses in terms of the Internet.

It's been said that the cost to Canada of the problem that we're trying to solve here is upwards of $3 billion a year in terms of the effect of spam and some of the things we're trying to stop with this legislation. It's a very significant problem, a problem that renders e-mail communication in many cases almost meaningless as we clog the pipelines that transfer information back and forth.

I guess I want to get a comment from Mr. Copeland and Mr. Misener on the economic potential of the Internet. I think it's suitable to close with a big-picture conversation about the economic potential of the Internet and how this ECPA will affect Canadians' ability to use the Internet to our long-term economic advantage.

Mr. Tom Copeland: In general, what we hope will come from the ECPA is a renewed confidence in the Internet and Internet communications as a tool for communications, for marketing, for e-commerce.

A lot of my ISP customers are afraid to go online and do anything. They don't want to purchase things. They don't want to do online banking. They've seen those e-mails come through that purport to be from the TD Bank or the Scotiabank or wherever. They're quite literally scared witless to go online and do anything.

I'm not sure we can put a number on the potential, but we're certainly seeing people avoiding the Internet now because of the issues that the ECPA can help solve.

Mr. Paul Misener: Thank you, Mr. Lake.

I would briefly add that Amazon.com established Amazon.ca about seven years ago. The whole purpose was to be able to better serve our Canadian customers, featuring Canadian content, particularly Canadian authors, musicians, and movies.

We want to ensure that we're able to communicate with them efficiently. This bill, we believe, would go a long way to removing the chaff so that communications are better between businesses and our customers.

We applaud your efforts here, we really do. My suggestions are not an overall criticism of the approach with the bill itself but just a few tweaks to make it better. I honestly believe these would improve the bill, but you've got a great piece of legislation before you already.

The Chair: Thank you very much, Mr. Misener.

We'll have a brief question from Mr. Rota in clarification before we wind up the meeting today.

● (1730)

[*Translation*]

Mr. Anthony Rota: Thank you very much, Mr. Chair.

My question is for Ms. Reed.

When you say that an individual or business can contact individuals to ask for their consent to contact them, it seems to me that we are inventing a new spam system. I think we are going to have some problems.

What kind of model do you have in mind? Could you describe it to us?

Ms. Geneviève Reed: Thank you for your question that will allow me to clarify matters. What I said was that given the notion of implicit, tacit consent, there is nothing stopping a company that has an existing business relationship with a customer from sending that customer within the allowable 18-month period an email asking him if he would like to receive additional information over the next few years. Then, the relationship could continue indefinitely or until such time as the consumer or the company decides to end it. This would be part of the express consent provision, to avoid a debate on whether the period of implied consent should be 18 months, two years, five years, eight years or twenty years. I think it's clear that any business can send out an email, once a business relationship has been established, and ask the customer for permission to continue sending emails.

Mr. Anthony Rota: So then, it would be within the context of an ongoing relationship, not a new one.

Ms. Geneviève Reed: Exactly.

The Chair: Thank you.

[*English*]

Thank you very much to our witnesses for appearing today.

We must adjourn; it's 5:30 p.m. However, just before we do, I have two points of information for committee members.

First, the clerk has distributed to members of the committee contact information for personnel or members who wish to suggest amendments to Bill C-27, which we are studying today. Before you submit your amendments to the clerk, so that all members can have them in both official languages, we strongly suggest that you consult with the legislative clerk and legislative counsel to ensure that the wording of your amendment is proper and in good form.

Secondly, we received an invitation from the International Astronautical Federation for a parliamentarian event in Taejon, Korea, concerning climate change. If any members, individually or in a larger group, are interested in attending this event, talk to the clerk and she can put you in touch with the international organization.

Without further ado, this meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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