



House of Commons  
CANADA

# Standing Committee on Industry, Science and Technology

---

INDU • NUMBER 026 • 2nd SESSION • 40th PARLIAMENT

---

EVIDENCE

**Tuesday, June 9, 2009**

—  
**Chair**

**The Honourable Michael Chong**

Also available on the Parliament of Canada Web Site at the following address:

**<http://www.parl.gc.ca>**

## Standing Committee on Industry, Science and Technology

Tuesday, June 9, 2009

• (1635)

[English]

**The Chair (Hon. Michael Chong (Wellington—Halton Hills, CPC)):** Good afternoon. Welcome to the Standing Committee on Industry, Science and Technology. This is Tuesday, June 9, 2009.

We are meeting today for an hour and a half, from 4:30 to 6 p.m., in order to study Bill C-27. We are televised.

Pursuant to the order of reference of Friday, May 8, 2009, we are studying 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.

We have appearing in front of us the Honourable Tony Clement, Minister of Industry, and two of his officials, Madame Helen McDonald, assistant deputy minister, spectrum, information technologies and telecommunications, and Mr. Richard Simpson, director general of the electronic commerce branch.

Welcome to all of you, and welcome as well to our Mexican delegation, who will be sitting in the audience, observing the Canadian parliamentary system at work. I welcome the Mexican delegation from the United Mexican States.

Without further ado, we'll begin with the minister for his opening comments with respect to this bill.

**Hon. Tony Clement (Minister of Industry):** Mr. Chairman, thank you, and thank you to members of the committee, of course, for the opportunity to meet the committee to discuss Bill C-27, the proposed electronic commerce protection act, or ECPA.

Joining me today we have two officials, Helen McDonald, the assistant deputy minister for spectrum, information technologies and telecommunications, and Mr. Richard Simpson, who is the director general of the electronic commerce branch of Industry Canada.

Mr. Chairman, in little more than a decade the Internet has become a critical medium, not only for communicating but also for competing in the global economy. It has become an essential part of the daily lives of Canadians, and essential to Canadian business.

[Translation]

However, in recent years, the Internet and the online economy have become more vulnerable with the rapid growth and increasing sophistication of spam and other online threats.

[English]

So the legislation before you today is about encouraging the growth of electronic commerce by ensuring business confidence and consumer trust in the online marketplace.

In 2007 one report estimated that the global cost of spam was at \$100 billion U.S. per year. Canada's share of this cost would be about \$3 billion. So unsolicited commercial e-mail is more than just a nuisance. Along with the development of associated threats like malware, spyware, phishing, and various viruses, worms, and trojans, spam has become a major disruption to the Internet and to the Canadian economy as a whole.

A growing chorus of voices across the nation has called for legislation to protect Canadians and the Canadian economy from spam.

[Translation]

The Canadian Chamber of Commerce has described spam as, and I quote, "a considerable burden not only to consumers, but to the business community."

Major industry associations, including the Canadian Marketing Association, the Canadian Bankers' Association, the Information Technology Association of Canada, and the Canadian Association of Internet Providers, have called for new laws to address this issue.

In October 2007, nine major industry representatives at the Canada Roundtable on the Future of the Internet Economy confirmed their support for legislative action to deal with spam and other threats on the Internet.

We have listened to their concerns, and those of millions of Canadians who have seen their email cluttered and clogged with spam and their computers compromised by the threats that spam causes when it slips into their software and disrupts their lives.

Mr. Chair, it is time to act.

[English]

We have debated this bill at second reading, and I am gratified to see the support this bill has received from both sides of the House. In fact, I must say that several parliamentarians have been calling for some time for legislation that would curb spam and other threats to the Internet and the online economy.

Senator Donald Oliver, for instance, in the other place, has introduced bills to combat spam. During last September's election campaign, the Prime Minister announced that if re-elected, the government would introduce anti-spam legislation.

I would also like to acknowledge Senator Goldstein and his bill, Bill S-220, which was introduced in the other place last February. I believe the bill before us improves upon his bill in that it empowers specific agencies, at royal assent, that would have the power to enforce the law, including the CRTC, the Competition Bureau, and the Office of the Privacy Commissioner. Like Bill S-220, this Commons bill also allows for a private right of action.

The honourable member for Pickering—Scarborough East emphasized the need for international action against spam. I would point out that the bill before us provides the CRTC, the Competition Bureau, and the Office of the Privacy Commissioner with the authority to work not only with one another, but also to work with their international counterparts. The honourable member for Pickering—Scarborough East also pointed out the importance of administrative monetary penalties that have teeth. I should mention to this committee that this bill provides for AMPs up to a maximum of \$1 million per violation for individuals and up to \$10 million for businesses.

During our debate in the House of Commons, other members from the Liberal benches spoke in favour of the principles of this bill. The honourable member from Scarborough—Rouge River told the House that he was pleased to see the private right of action included in the bill. This right would allow users and businesses to take civil action against anyone who violates the act. This remedy has been very effective in the United States, Mr. Chairman, and is one example of how we have adopted the best practices from around the world.

The NDP have a solid history of favouring anti-spam legislation. Last fall their election platform contained a commitment to “Combat identity theft and control online computer fraud against...consumers and seniors” and against “spamming and phishing”. During second reading, the honourable member for Nanaimo—Cowichan reminded us of spam's impact on the productivity of Canadian workers. She reminded us that Canada is the only G-7 country without anti-spam legislation, and I would like to assure her, through you, that the bill before us benefits from the best practices of the jurisdictions that have gone before us in introducing anti-spam laws.

The honourable member for Timmins—James Bay has been an outspoken champion in protecting Canadians from spam. When speaking to this bill, he expressed concern about the implications Bill C-27 will have for the national do-not-call list. The honourable member for Scarborough—Rouge River, also from the Liberal Party, raised concerns about the national do-not-call list as well.

I should mention to this committee that the do-not-call list is up and running, and it is effective; over six million Canadians have signed up. At this point in time we always have the ability to review these things, but we would like to see the DNCL continue for the time being, and we do not want to shelve it with this legislation at this particular moment in time.

As my parliamentary secretary indicated during second reading debate, Bill C-27 will not abolish the do-not-call list. In fact, subclause 6(7) enhances do-not-call lists because it carves out telemarketing by exempting interactive voice communications, facsimiles, and voice recordings to telephone accounts from the application of the act.

It's well known, however, that with the convergence of technologies, the distinction between voice telephony and Internet-carried communications, for all intents and purposes, is disappearing. Clauses 84 to 86, which could repeal section 41 of the Telecommunications Act and the do-not-call list, would not be proclaimed by the government until it is necessary to deal with such changes. That is to say, we are going to continue to monitor how this particular aspect of the bill changes over time and we will have the flexibility to react to those changes.

The Bloc spoke in favour of the principles of this bill. The honourable member for Chicoutimi—Le Fjord reminded us of the increase in the amount of spam and wondered whether businesses were changing the way they contact consumers.

● (1640)

Before the debate adjourned on May 7, I believe the honourable member for Jeanne-Le Ber was about to make a point about the difficulty of policing the Internet. It's unfortunate that the debate was cut off at that moment, because I appreciate the concerns about the challenge of enforcement when communications technologies know no borders. However, I'd like to assure the committee that it is indeed possible for anti-spam laws to have a huge impact.

In Australia, for example, after the Spam Act came into effect, the proportion of global spam originating from that country was greatly reduced. Some major spammers, particularly pornographic spammers, closed their Australian operations altogether.

Mr. Chairman, during second reading, two themes recurred in most of the interventions. First of all, all parties support the intent of this bill. We just want to ensure that we get the details right. Second, many speakers said they looked forward to examining the bill in greater detail here at committee.

I'm pleased that we have the opportunity now to do just that. I encourage members to read it through, to understand the intent, and to ask questions. You'll see that the legislation in front of you is solid and considered and that it will make a big difference in protecting Canadians in the online marketplace.

On that note, Mr. Chair, I'll be very pleased to hear from the committee members. If there are more technical aspects to this bill, we have departmental officials to answer your questions and clarify those more technical provisions that may require explanation.

Thank you.

● (1645)

**The Chair:** Thank you very much, Minister. We'll have about an hour and fifteen minutes of questions and comments from members, beginning with Mr. Garneau.

**Mr. Marc Garneau (Westmount—Ville-Marie, Lib.):** Thank you, Mr. Chair.

First of all, I'd like to thank the minister for his comments, and I would like to reiterate to him in no uncertain terms that the Liberal Party welcomes Bill C-27 in the interests of combatting spam. There's no question that we're very glad to see this as a follow-up to the task force that rendered its report back in 2005.

However, having said that, I must mention some very significant concerns about Bill C-27 that have been expressed to me in the course of the last few weeks.

If I could try to summarize, the net has been cast in order to eliminate spam, but it has been cast in a very broad manner. The devil is in the details, and there are significant concerns about its having some negative effects. Casting the net so broadly has also left certain definitions so general that the interpretation of something as simple as a computer program can be taken in a number of ways. With respect to the anti-spam provisions, the scope is too broad at this point, specifically with respect to the consent provisions contained in the bill, and exclusions are too narrow. The unsubscribed requirements are unworkable, and this could have a chill on legitimate commercial speech and e-commerce.

We want to help fix that, because the anti-spam bill is a good thing, but we have a lot of work in front of us in order to address some of the specific concerns that have been expressed to us by people who also want to see Bill C-27 come into play.

As a first question, I assume the team that put together the bill has consulted legislation from other countries. There are recent examples of legislation in other countries, and you mentioned Australia; Australia is one example, and New Zealand is another. Have other countries' legislation been consulted in the process of putting this bill together? At first sight, some of what they have done appears to address many of the concerns that have been expressed to me by various organizations.

**Hon. Tony Clement:** Thank you. I'll just pass it over to Helen.

**Ms. Helen McDonald (Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications, Department of Industry):** The United States has also been consulted, and that is where we got the notion for the private right of action.

**Mr. Marc Garneau:** How about New Zealand and Australia?

**Ms. Helen McDonald:** We looked at New Zealand and Australia; yes, absolutely.

**Mr. Marc Garneau:** I would suggest that we need to look at some of the things they have done that get around some of the objections with respect to the scope being too broad. In terms of defining some of the words that are used in this legislation, let me bring up a couple of examples.

One has to do with extraterritorial provisions. The anti-spam and message-altering provisions that exist at the moment apply to any message when a computer system located in Canada is used to send, route, or access the electronic message. The key word here is "route". As you know, the way the Internet works is that we can have messages flowing through Canadian computer systems that don't originate in Canada and are not ultimately going to end up in Canada. The use of the word "route" is problematic in this particular case. That is an example that I think perhaps you may want to address. We need to address it.

**The Chair:** Mr. Simpson, go ahead.

**Mr. Richard Simpson (Director General, Electronic Commerce Branch, Department of Industry):** Thank you.

It certainly is a valid point that spam is a global problem and that legislation therefore has to take account of international arrangements, as well as put forward the right legal powers to tackle spam domestically. The example of Australia is a good one. They've tried to make sure their domestic rules, through an Australian link, apply with respect to international origins of spam.

With respect to the point about Internet transmissions and how those are global because of the nature of the Internet—they can't be sourced in any one country, but they go through the whole network and then arrive at their destination, which could be anywhere—that's true. But the bill does provide for a specific exemption for telecommunication service providers when they're performing the function of telecommunications. Therefore, it's a waiver, if I can use that term, for the function of carriage, and certainly the example you use about the Internet would be captured by that.

Hopefully, we won't get caught by a specific transmission function that is going to be subject to any of these anti-spam provisions, certainly not as it relates to telecommunication service providers.

● (1650)

**Mr. Marc Garneau:** Getting back to defining some of the terminology here, when we think of HTML files that are regularly used in accessing websites, or JavaScript, which is another common example, or updating programs that some of us use, for example, Symantec antivirus software, those would not be looked upon as spam, and yet, by the definitions that exist within clause 8, I believe, they could be looked upon as being spam.

So again, that is something that needs to be tightened up. It needs to be clarified so that it doesn't create serious impediments to legitimate users.

**Hon. Tony Clement:** No. We have noted that particular concern about clause 8, I can tell you, Mr. Garneau. I guess what we're trying to do is provide the right balance. Clearly, if you're getting an upgrade, if there's an implied consent or some other mechanism so that we can have these reinstallations or upgrades in our computers, that's an obvious legitimate practice.

We have to make sure that is legitimate, but we don't want to leave the barn door so wide open that the bad guys can use that as the way to get the spam in. We're prepared to work with you to get the right kind of language that will balance this off appropriately.

**The Chair:** Thank you, Mr. Minister.

Thank you, Mr. Garneau.

Monsieur Bouchard.

[Translation]

**Mr. Robert Bouchard (Chicoutimi—Le Fjord, BQ):** Thank you, Mr. Chair.

First of all, Minister, you know that the Bloc Québécois supported the bill at second reading. As a committee, we want to hear from the various witnesses, we want to know their opinions and listen to what they have to say.

This bill will affect three bodies: the CRTC, the Competition Bureau and the Office of the Privacy Commissioner. I would like you to describe what role each will play, as well as the kind of coordination they will engage in. How will they coordinate their efforts while being effective and efficient? You have three major players. Will these organizations keep up a dialogue? I would like you to speak to their respective roles and to how users and consumers will benefit.

**Hon. Tony Clement:** Thank you.

Ms. McDonald and Mr. Simpson may have something to add, but I would like to say a few things.

In its final report, the Task Force on Spam recommends that, and I quote, “enforcement of new legislative provisions addressing spam should be undertaken by existing agencies.” Of course, that means that the CRTC, the Competition Bureau and the Office of the Privacy Commissioner are organizations that we can use to protect the public from spam. Similar legislation has already been passed in other countries including Australia, New Zealand and the United Kingdom.

Ms. McDonald may have something to add.

• (1655)

[English]

**Ms. Helen McDonald:** With this law we are very much trying to build on the existing mandates and competencies of these three agencies. Therefore, you could look at the CRTC as the major organization charged with stopping the spread of spam and the use of spyware.

When we look at the other two agencies, we are trying to build on their mandates to make sure the Competition Bureau can apply its rules and its role around misleading and deceptive advertising in a computer environment. So we've enlarged their mandate, but they're using their existing tools.

With the Privacy Commissioner, we want to make sure she has the tools to prevent electronic lists from being created that can be then farmed and used for spam.

For the Privacy Commissioner and for the Competition Bureau, they have existing mandates. We're extending their mandates, but they're using their existing tool set. With the CRTC, we are creating, in a sense, another tribunal that will be able to look at violations with respect to spam and take action appropriately.

To ensure that coordination that you were concerned about, we are proposing a small organization within Industry Canada that would make sure that the three organizations are working together effectively to achieve the purposes of this legislation. It will make sure that when we look at our situation more broadly, Canada is continuing to not be a safe haven for spam, but a spam-free environment. So there will be a national coordinating body within Industry Canada that will make sure the three work together effectively.

There is also a spam reporting centre proposed where people could send reports of spam. It would serve all three agencies to prevent unnecessary duplication.

[Translation]

**Mr. Robert Bouchard:** As you know, in some cases, spam makes it very difficult to use the Internet. It really hinders the effectiveness and efficiency of email.

Your bill excludes telemarketing so that it is not subject to the legislation. From what I understand about telemarketing, it is solicitation on the Internet. So how can this bill protect against all solicitation of that nature? The first thing people do in the morning is clean their computers because of all the spam they receive. If the bill excludes telemarketing, that means that users, consumers, will still receive telemarketing messages they do not need.

I would like to hear your thoughts on that. How can you ensure that users and consumers will be protected when they are on the Internet at their workstations?

**Hon. Tony Clement:** Right now, technologies are converging, and in the future, it will be possible to have a convergence of the telephone and the Internet. But for the time being, we have the national do not call list for the telephone. For other means of communication, such as the Internet, our legislation establishes a system.

• (1700)

[English]

**Ms. Helen McDonald:** In his remarks, I think the minister pointed to why the do-not-call list should continue. It's a fairly new regime. It's still finding its feet, and we believe it can be effective.

You are talking or are worried about other spam, but telemarketing usually refers to a voice-to-voice communication. That is what is covered by the do-not-call list. If you're worried about text messaging on cellphones, that's not voice-to-voice. That's people sending messages by the Internet. That would be covered by this. Spam, which is just computer-generated electronic e-mails—as long as they are unsolicited commercial messages—would be covered by this. There are two regimes being maintained for the time being.

As the minister said, as one looks into the future, when people start moving to computer-generated voices that leave messages on your home phone, it becomes complex. The way the bill is structured, the government would have the opportunity to react quickly.

**The Chair:** Thank you, Madam McDonald.

[Translation]

Thank you, Mr. Bouchard.

Mr. Lake.

[English]

**Mr. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC):** Thank you, Mr. Chair.

Thank you, Mr. Minister. Obviously when we are looking at an issue like this, we have a bit of a challenge to find, as with all legislation, a balanced approach. In this case, I think the challenge is to find a balance between catching the bad guys, the most malignant forms of spam, and yet still allowing businesses to contact their legitimate clients without worries of someone knocking on their door to take them away.

Can you maybe clarify a little bit how this bill sort of captures that balance, maybe from the side of addressing these concerns that might be expressed by the business community?

**Hon. Tony Clement:** Certainly. I think, for instance, there are legitimate e-mail marketers who want to communicate with their clientele. What we've tried to do is create both explicit consent and implied consent in those situations when there's a pre-existing business relationship.

I used to be in the legal beagle business. Let's say you've got clients. You're a lawyer with clients, and you want to send them updates about particular aspects of changes in the law; let's say anti-spam legislation, for instance. Obviously, there's a pre-existing business relationship, and those kinds of things do imply some consent by the receiver of that information, by the consumer of that information. We're not trying to interfere with the legitimate e-mail practices of legitimate businesses, of course.

We have the implied consent mentioned in the legislation. We can further hone that down in the regulations as well, where we can describe further circumstances where marketers can rely on implied consent. Again, we're not trying to interfere with the existing business relationships. We're trying to deal with bad guys who right now can drive a truck through the open barn door because there's no regulation.

• (1705)

**Mr. Mike Lake:** I have a question for Ms. McDonald or Mr. Simpson.

Often when you go through legislation like this, once you put it out, there are folks who want to comment on it, express concerns, or get some clarification. I imagine you've had some folks comment or contact you regarding this. What kinds of common concerns have been expressed at this point?

**Ms. Helen McDonald:** There are concerns around the consent regime. People ask if we have the balance right and how implied consent would be considered.

As the minister said, you don't want to open the door too broadly. Therefore, we've tried to strike a balance to ensure that a pre-existing business relationship could be such that if I've expressed interest in a product or service, that's an implied consent. We hope that would be sufficient. We look for your investigations on that.

I think Mr. Garneau raised the question about the computer programs and if there is an issue with the downloading of software to keep your computer virus-free. The concern is if we have the wording a little too restrictive on that. Should that be a softer, more implied consent, or an explicit consent program by program? I think those are the two major concerns we have heard.

**Mr. Mike Lake:** In terms of the other countries' anti-spam legislation that's referred to, I understand it's been a real success in

those countries. Are there any lessons to be learned, any response that can be given or experience drawn upon, based on the knowledge we have of those countries' legislation that might address some of the concerns that some stakeholders might have?

**Ms. Helen McDonald:** I'm going to ask Richard to answer that, given his greater experience in putting this together, but also because he interacts more closely with other countries with similar regimes.

**Mr. Richard Simpson:** Thank you.

The one common denominator that has come out of work in the Organisation for Economic Co-operation and Development, which started an examination of spam and other harmful activity on the Internet a few years ago, was that you need a combination of tools, legal and technical, to deal with spam. I think that's the first lesson.

The legislative side of it, which I think has been recognized in the work that we've been doing on spam, is one of the important pieces of that toolkit approach that we need. I think you'll find that every country that has a successful result from their work on spam—for example, Australia—has a toolkit approach. In fact, Australia, like Canada, talked about toolkits at the same time the OECD promoted that particular approach.

Australia has taken an approach towards spam that, like this bill, is based on the concept of consent. As I mentioned before, they have looked at it as a domestic regime that has to work in combination with international arrangements to deal with spamming. Another similarity to Bill C-27 is that the Australians do use their communications regulator as well to deal with some aspects of spam.

Interestingly, Australia is a country that formally reviewed its anti-spam legislation in 2006 after about three years in operation. They found out from the data that because of the legislative arrangements they put in place, they had reduced Australia's contribution, if I can use that word, to global spam to something that was well down in the list. It was off the top 20 list of spam-originating countries. I think that's a good example of how that toolkit approach has been effective in that one country.

**The Chair:** Thank you, Mr. Simpson.

Thank you, Mr. Lake.

Mr. Masse.

**Mr. Brian Masse (Windsor West, NDP):** Thank you, Mr. Chair.

Thank you, Mr. Minister, for being here. Thanks for noting the New Democratic policy from the last platform. Feel free to act on our position on net neutrality and employment insurance reform as well, if you like.

**Voices:** Oh, oh!

**Mr. Brian Masse:** There are other suggestions on priorities.

Mr. Minister, I know you heard these problems with regard to some of the types of issues being raised here. Do you now plan to bring amendments to this legislation, or right now is it one that you want to pass in its current form?

• (1710)

**Hon. Tony Clement:** I take this committee seriously. If you have some common-sense suggestions that would fit into what our aspirations are for this particular bill, then I think we're prepared to look at that, absolutely. I encourage you to do that.

The only thing I would say, and I guess Mr. Garneau raised this a little bit, is that we do consider this economic legislation. There is a \$3-billion-a-year effect on business in this country. I think we should hunker down at committee and come up with some positive changes that will make this a better bill.

I don't want to stretch this out too long, because, quite frankly, we're costing businesses in our country money, and we're the only country in the G-7 that doesn't have anti-spam legislation. I think it's incumbent upon us to get the shoulder to the wheel and get this done.

**Mr. Brian Masse:** I appreciate that. I agree, as long as we can do the proper bill, and then we could also move on to my private member's bill, Bill C-273.

**Voices:** Oh, oh!

**Hon. Tony Clement:** This is a paid political announcement.

**Mr. Brian Masse:** Yes.

But I do want to run through a couple of scenarios, to be clear here. I want to make sure I understand the interpretations that are happening, as well as this information coming to us. For example, would automatic updates be considered spam under this bill if it's passed?

**Hon. Tony Clement:** Do you mean with the pre-existing relationship? That's what we're saying. We would like that to be part of implied consent.

Helen, do you want to talk about that?

**Mr. Brian Masse:** Yes, as it currently stands in terms of interpretation. I have a couple of scenarios here.

**Ms. Helen McDonald:** It's clearly written as express consent for program modifications.

**Mr. Brian Masse:** So right now that would be spam, then, under this?

**Ms. Helen McDonald:** No, I haven't said that. I'm simply saying that the spam itself allows for implied and express consent. The modification of your computer program requires express consent the way it's written now. It does it kind of program by program; I imagine there are easily ways in your contract, whether that's electronic or paper, with your security software provider. One could provide that express consent for "yes, I want the automatic updates", and so on.

So I would not see that as problematic. I think what we're trying to make sure of is the wording we have for the combination of you agreeing to every explicit program and express consent—that we have it worded correctly.

**Mr. Brian Masse:** That could be through regulations and licensing.

Very quickly, then, let's say, for example, that a new software company wants to communicate with other software distributors and

all that. Would they be able to send out a message to everyone within their own field of software development or would that be considered spam? Would they have to rely on traditional mail to contact people they haven't had contact with before in the business but who are integral for developing that industry?

**Ms. Helen McDonald:** There's a provision for business-to-business e-mail—

**Mr. Brian Masse:** Even if they have no pre-existing relationship?

**Ms. Helen McDonald:** Yes.

**Mr. Brian Masse:** Okay.

As well, very quickly, I want to touch on the do-not-call list. What other types of changes do you foresee? One of the things that I tried to get on the do-not-call list last time was the computerized "ghost call" that happens to individuals first, to determine whether you're home or not; then it hangs up right away. That amendment was defeated, unfortunately, when we passed that bill.

Would this provide an opportunity for you to address that issue? That's becoming more and more of a problem. You're at home, they do the first phone call, and if you pick it up, then it's blank, it's dead air. From there, the telephone solicitor or the operative then calls you back immediately, knowing that the person is at home. Would there be a remedy in this bill here?

**Hon. Tony Clement:** I would say no, because our bill is dealing with electronic communications, not using telephones for a medium.

But it's becoming difficult to separate these things out. That's what I was trying to signal in my remarks. We have a contract with Bell right now. They run the do-not-call list, so I want to obviously let that contract kind of run, and this bill gives us an opportunity, then, to start to see if things have converged to such an extent that you can't really chunk out telephony on one end and the electronic on the other. Then we will have an ability to tuck everything into the same kind of regime.

• (1715)

**Mr. Brian Masse:** Okay. I think there's some fear being expressed out there that this potentially could open up, and that the do-not-call list would be vulnerable.

**Hon. Tony Clement:** I don't think so. I think it's expressly excluded, but it gives us a chance to sort of tuck it in if we so choose.

**Ms. Helen McDonald:** I'm just trying to be precise here. The two-way voice communications is the carve-out we've made to keep the do-not-call list whole. I'm not familiar enough with what a ghost call is. Would that be a computer-generated call?

**Mr. Brian Masse:** They often use a computer system. Somebody calls you first for telephone marketing and they hang up on you. Often they use a computerized system to pull the numbers up, and then if you're home, they call again.



**Hon. Tony Clement:** I know those calls, believe me. We're all victims of those calls. I'm waiting to strangle the Captain Stubing guy with the wonderful ship in the background tooting its horn. That's the one that bugs me the most.

**Ms. Helen McDonald:** We've had the clarification. The ghost call would be covered under the do-not-call list.

**Hon. Tony Clement:** Oh, lovely. It's under the do-not-call list.

**Mr. Brian Masse:** Thank you.

**The Chair:** Thank you, Mr. Masse.

Mr. Rota.

**Mr. Anthony Rota (Nipissing—Timiskaming, Lib.):** Thank you, Mr. Chair, and thank you, Mr. Minister, for coming out today.

I think spam is something that concerns all of us, and we want to see some kind of legislation out there that would prevent unwanted spam.

One of the things you mentioned earlier in your speech was that you wanted to encourage the growth of electronic commerce. I think that's something that has to be encouraged, and it's a wave of the future. One of the things that has come up in discussions with some of the people who are directly affected by this legislation is that the legislation doesn't zero in on one activity or certain activities and stop them. It basically throws a wide net out there and stops everything. Basically, everything is illegal except for a small list of activities that are permitted.

That's the way it was described to me by someone who's affected directly by this. I was wondering if you can comment on that, because in this changing world of electronics, we have new products, new actions, and new ways of doing business coming about on a regular basis.

So, first, could you maybe comment on this wide net that allows only certain activities through? And second, with the intervention of new activities or new ways of doing business, how long do you see it taking to make a change, so that it can adapt to a changing world?

**Hon. Tony Clement:** Thank you for the question.

Certainly, if you look at the structure under clause 6, you're quite right. It's saying that no person shall do this unless they fit into the category. I would argue that that's the appropriate way of doing it, for the following reason.

This area, obviously, is changing rapidly by the year, by the month, by the week, and if we tried to itemize the things that were accepted rather than having a blanket prohibition, we'd be getting into a situation where the legislation would almost be out of date by the time we got around to getting royal assent. That would be my fear. You'd be constantly seeking exceptions to the general rule of openness—which would be the opposite of this—because other methodologies would come forward that would be legitimate methodologies, or, in your case, other things would come forward that are bad—some new form of malware, some new form of spam—and then we'd have to plug the hole and say no, that one's excluded too.

So I think it's better to exclude everything and say no, everything's excluded. Assume it's spam or malware, unless you fit into what we

know is legitimate commerce or legitimate communication under this particular bill.

**Mr. Anthony Rota:** You can understand the concern, though. If somebody's doing business and they say okay, we're going to do business a certain way, and they're restricted because it's not part of the legislation, and it's not defined, that's a real concern.

I just had someone from the real estate board asking what would happen if a certain real estate agent heard through a friend that an acquaintance of theirs was looking for a house. If they had a house for sale within their portfolio, it would be illegal for them to contact that person to offer them a house or to say, "Look, I understand you're looking for a house, and is this something that would interest you?" Would that be something that would be blocked?

• (1720)

**Ms. Helen McDonald:** I'm sure there are many ways in which the real estate agent on this particular issue could express it or make it known through a friend. We're talking more about the mass sending of the kind of e-mail that—

**Mr. Anthony Rota:** You're telling me that the real estate agent would be caught in this vast net that covers absolutely everything if it's not defined. If it's not defined in there, that person can't do business. You're preventing someone from using a tool that would be very useful to them to do business.

**Ms. Helen McDonald:** I don't think we've quite worked out the precise example, not being at the meeting, of how they positioned this—whether there was an implied consent like "I know a real estate agent; if you like, he can call."

**Mr. Anthony Rota:** Basically what happens is someone tells you they have a friend who's looking for a house. If that person gets an e-mail from you, all of a sudden that's illegal. That takes the place of—

**Hon. Tony Clement:** We'll get back to you.

**The Chair:** I think Mr. Simpson might have something to add to this.

Mr. Simpson.

**Hon. Tony Clement:** Just looking at it quickly, I think at the very least you have the ability under regulations to deal with some of these examples. Paragraph 6(5)(c) would give us the power to say these are acceptable commercial activities, these cases.

**Mr. Anthony Rota:** You know as well as I do, Mr. Minister, through you, Mr. Chair, that around Parliament things don't happen instantaneously. We find holes and it takes forever to change them. Meanwhile, industry comes to a grinding halt because we have tools we can't use. That is my concern with this legislation. It's the fact that it has a very wide net that impedes business. When I look at what's going on with the economy today, the last thing we need is another break in the economy. In going through Bill C-27, that's what keeps coming up. I feel this legislation has been put together in haste and there are problems.

**Hon. Tony Clement:** This legislation has been kicking around this department for a good long time. Previous governments have tried to do legislation like this but have never got around to it. I would reject the idea that this is put together in haste.

I would say this, however. You can come up with examples and I won't know the answer immediately to a particular example. But I will say that if you want a situation where everything is open unless it's specifically excluded, then the bad guys will find a way to be excluded and this legislation will not work and it will not protect anybody. It will not protect commerce, it will not protect business, and it will not protect consumers. I still abide by the philosophy that you exclude everything unless it is a legitimate form of communication, in which case it's fine. I think that's a better way of looking at it.

**The Chair:** Thank you, Minister.

Thank you, Mr. Rota, for those questions.

Mr. Wallace.

**Mr. Mike Wallace (Burlington, CPC):** Thank you, Mr. Chair.

I thank you, Minister, for coming, and for having folks here.

Can you follow up a little on Mr. Rota's example? I think Mr. Rota's example is exactly what we're trying to resolve in this. If I'm a homeowner talking to my friend about maybe moving and I get a slew of unsolicited e-mails from real estate agents, I'm not happy about it. That's the whole idea.

I don't have any problem—that is my privacy and there are other ways for real estate agents. Now if I give permission to my friend to tell that real estate agent to call me, e-mail me, mail to me, or come to my door, that is a different story. Without permission or consent, I don't agree with it.

I'm happy with the legislation. It has been kicked around for a while. Could you give me a sense of whether that's a year, two years, or three years? Do you have any idea how long you've been working on this? I don't mean you, Minister, but the staff.

**Mr. Richard Simpson:** The origins of the bill actually go back to the work of the spam task force, as one of the members mentioned.

• (1725)

**Mr. Mike Wallace:** How long ago was that?

**Mr. Richard Simpson:** It was in 2004.

**Mr. Mike Wallace:** That was in 2004. Thank you very much. I don't need more information.

This has been working around. We have had support from our colleagues. I know there are some issues. My question about the issues that you've heard today really breaks down to two, as far as I can tell from the people I've seen and the reading I've done.

First, if you have a software package and they do an overnight update on it, and they drop cookies down or they drop something on there, is that covered off? I need to know, do you need word changes to this bill, or do we pass it the way it is and make a commitment to fix that during regulation? That's my first question.

The second area that I think you've clarified considerably is that we will not give royal assent or declare, whatever you call it, the

section to deal with...because I think one clause, clause 86, actually repeals the section that has the do-not-call list in there. So if we don't declare it, or whatever we call it, it will stay in abeyance until we need it.

We had a great example at our own committee, of most of these members who are here today, of a country in Africa where you don't need a card of any sort to do your banking because they do it by phone. Who knows what's coming next in this country or any other country in terms of spam? That's fully integrated with their phone, and that could be coming here—those kinds of things.

Is there specific wording that you've been working on or that you need changed at committee? I don't even know if we can do it at committee, but from a process point of view, how...? I'm a little bit with Mr. Masse on this. I'd like to see this passed relatively quickly. We have our witnesses in the next few days. I think we should get on with this process. It has been hanging around way too long. That's why people get frustrated with government, because we take forever to find issues when we need to move on to other projects.

I'm happy to debate Mr. Masse's bill when it eventually comes back here.

**Hon. Tony Clement:** Let me answer the question there. We talked a little bit about clause 8 and the anti-spyware provisions, and we talked about express consent and installation of computer programs, whether there's consent or no consent, that kind of thing. Certainly under subclause 10(2), for instance, there's some language there that could perhaps be tightened up a little bit that would be—

**Mr. Mike Wallace:** Are you providing us with that wording, or do we make that up on the fly? What happens? That's my question.

**Ms. Helen McDonald:** We're looking at that wording ourselves because we're also hearing from some groups asking if that would capture the security upgrades and so on. So we're looking at that, but I think, depending on the witnesses you're calling before committee, they may also be probing into that.

**Mr. Mike Wallace:** Okay. I appreciate that.

For clarification, my understanding, based on my review of this—I think it's clause 6, but correct me if I'm wrong—is that business to business, not business to consumer but business to business, is actually exempt, virtually exempt. So if company A wants to talk to company B, who is in the software business, or anybody in the software business, they can send their unsolicited e-mail to absolutely everybody and this legislation does not cover that. Is that a correct statement?

**Hon. Tony Clement:** That is correct.

**Mr. Mike Wallace:** Okay.

**Mr. Richard Simpson:** Clause 6, yes, you're correct. Paragraph 6 (5)(b) talks about an exception when the e-mail is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity. So I simply point out the qualification there, that this has to be a commercial activity in which there is a purpose that is, I guess, mutually shared between the two individuals. You can't necessarily, because it's a commercial activity, then send it out to every business in Canada.

**Mr. Mike Wallace:** Right.

**The Chair:** Thank you, Mr. Simpson. Thank you, Mr. Wallace.

Monsieur Bouchard.

[*Translation*]

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

Minister, since the Internet is a worldwide network, spam can come from Quebec, Canada or abroad. Earlier we talked about three organizations: the CRTC, the Office of the Privacy Commissioner and the Competition Bureau. Who will have the authority to intervene?

Say I am fed up with receiving emails from outside Canada, and I did not give my consent to receive spam. Which organization do I complain to? What will they do about the spam I receive from abroad? Can they take any effective measures? Can these organizations take action outside Canada?

• (1730)

**Hon. Tony Clement:** Yes, it is more effective than what we have right now. This bill contains a provision whereby the CRTC will have the authority, as will the Competition Bureau and the Office of the Privacy Commissioner, to share information and evidence with their international counterparts, if similar laws exist in other countries. In addition, Interpol handles these matters in the international arena. It is possible to have partnerships on this issue. Right now, it is hard for other countries to establish a partnership with Canada because, without a law, there is no way for them to work with us.

**Mr. Robert Bouchard:** Thank you. I completely understand. So, in Canada, the legislation would undoubtedly give more authority and be more effective, but abroad, it would be subject to agreements and partnerships with other countries. So it still needs to be done.

I want to discuss something else. We know that e-commerce is important. Many merchants offer services on the Internet. Once the legislation is in effect, every merchant wanting to offer a service to Internet users will first have to obtain permission to contact them. Once the legislation is in effect, someone who receives spam and who has not previously consented to receiving that spam will be able to complain.

Which organization can that person complain to? What will happen? Their complaint will be received, and an investigation will be conducted. Will the person be notified of the outcome?

[*English*]

**Ms. Helen McDonald:** If we're talking about spam, then you could either complain to the CRTC or you could complain to the spam reporting centre, an organization that we have yet to set up, but it would be complementary to this legislation. So if you don't know

who to phone, don't worry about it. You can call or e-mail the spam reporting centre, and between the three organizations, they will figure out who is best positioned to take action on this.

As you know, a lot of these organizations—at least the CRTC does—carry on quasi-public proceedings. You would find out what is happening to your complaint from them. They also have the ability to publish the results when they find someone has violated the act and there has been a penalty extracted. They have the ability to publish that information for you as well, so you can see that they are being effective.

**The Chair:** Thank you, Ms. McDonald.

*Merci, Monsieur Bouchard.*

We now have Mr. Van Kesteren.

**Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC):** Thank you, Mr. Chair.

Thank you, Minister, for appearing before us.

Mr. Minister, we're right in the middle of a very significant global economic crisis, and I'm curious why the government would choose this time to introduce this legislation. How will fighting spam contribute to Canada's economic recovery? In that light, how important is it that we get this legislation passed as quickly as possible?

• (1735)

**Hon. Tony Clement:** Thank you.

Certainly, I respect this committee's willingness to tackle this legislation with us and to work with us to get the best legislation possible, but as I mentioned at the beginning, this spam costs Canadian businesses \$3 billion a year. There's the cost of guarding against spam, of course. As businesses and consumers, we all get our anti-virus patches and continue the war that keeps expanding to the next level with the spammers, and that requires constant vigilance and upgrades and so on.

So it's expensive. I'm not saying it's all going to disappear with this legislation. Obviously, spammers, bad guys, are going to be around trying to get around the rules, but the fact of the matter is there's a big gaping hole in the world right now, and it's Canada. If you look at the top 25 spammers in the world, something like a third of them are in Canada. They're based in Canada because it's the wild west here.

So I think we have to do our part internationally. It's hard for us to work with Interpol. As I said to Monsieur Bouchard, it's hard for us to work with them if we have no legislation. We cannot come to the table with clean hands in that situation. We're not seen as a good partner right now. So we have to have legislation; it has to be as effective as possible.

Is it going to eliminate everything? No, I'm not here to say that. But the experiences of other countries has been...Australia is a good example. When they passed legislation, when they enforced their legislation, their indigenous spam, if you will, dropped by 40%. So it can have an impact, and that means savings for businesses and less frustration for consumers, and that's what we want.

Now is the best time to do this, in the wake of the world economic downturn.

**Mr. Dave Van Kesteren:** I suppose that leads me to the next part of my question: stakeholders. What kind of response have you received from stakeholders and the business community in general? Have they been supportive of this legislation?

**Hon. Tony Clement:** We've had very positive feedback from the Canadian Marketing Association, for instance. I'm sure there's a whole list here somewhere.

Do you have it there, Helen?

**Ms. Helen McDonald:** The Canadian Association of Internet Providers has reacted quite favourably to this. The Canadian Chamber of Commerce has reacted quite well. Mr. Perrin Beatty put out a statement after the bill was tabled.

**Hon. Tony Clement:** Right.

There's a quote from a Telus spokesperson, who says, "...it provides a legal framework to stop Canadian-based spammers from bombarding Canadians with unsolicited messages and potentially dangerous malware." Mr. Beatty said that he's been pressing the government for years. In a quote he says: "I'm pleased that the government is acting to make the Internet safer and more secure."

That's the general impression out there. Certainly, as I say, if there's a way we can improve this in an expedited manner, I think we're willing to do that as well. But at some point the process of debate must stop. We've had that for years. We actually have to pass some legislation.

**Mr. Dave Van Kesteren:** What about a review date? Is there an automatic review date? Is it three years? Five years?

**Ms. Helen McDonald:** No.

**Mr. Dave Van Kesteren:** Would it help to have a review? Is it something we should introduce?

**Hon. Tony Clement:** If the committee felt strongly that that's important, I'm not going to throw myself in front of that train. If you think it's important to have good legislation, that's fine by us.

**Mr. Dave Van Kesteren:** Okay. Thank you, sir. That's all.

**The Chair:** Thank you, Mr. Van Kesteren.

Thank you, Minister.

Mr. Masse.

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

That's one of the things we actually added. We augmented the do-not-call list for the review as well. Especially as the program is in its infancy, it has unintended consequences, regardless of all the things we do. Sometimes that's good to bring back, so I'm glad it was raised.

I want to go back to the real estate example because I just want to make sure I'm clear as to how this works, and also about another scenario that might evolve. If we don't have the answer for this today, it's fine. I'd just like to eventually get this, and when we have some witnesses it will help.

From what we understand right now, if you sign on with a real estate agent to find a house or sell your house, you can have an agreement there where the real estate agent, or anybody in his actual agency, could then send an e-mail to you if that scenario comes up where another agent at the same agency wants to send you information related to a search for a house or the sale of your current house. Could that be written as part of the agreement when you sign up? To answer that, what they couldn't do is then provide it to some other real estate agent from another entirely different agency.

So could you have that relationship so you have it with not only the one agent in the company but with all the agents who have signed on to their entire policies and so forth, and then exclude, I guess, the separate ones, like his buddy whom you just talked to down the road, or something like that?

• (1740)

**Ms. Helen McDonald:** I don't know enough about real estate to know whether you're signing on with a specific agent, and any of the agents working for the same company are all working towards the same goal. Perhaps during the discussions, as you try to establish this relationship with the realtor, that would be covered and it would be part of implied consent. I think you used the word "written". It would not require that you have a formal agreement with them as to who could e-mail or call or not. I think it could come up in a discussion, and as long as it was understood, then it would be a form of implied consent that we'd ask whether, if our sister company or someone else had places in this area, you'd be interested in hearing about that.

**Mr. Brian Masse:** Yes, because it brings up a further scenario. You have businesses like real estate agents or insurance agents and car dealers, for example, where they create their own databases of people they've been customers with. With this bill, what would happen if they left? This often happens in those occupations, that they move from either a provider or a company on a regular basis, every couple of years; it's not uncommon. Would they then have the ability to re-contact all their contacts, if perhaps the person has agreed, under the scenario of the person's being at a particular agency? At the same time, you often actually... I use the same real estate agent we've always had, but the person has changed to different companies.

Once again, we don't have these scenarios now, but I think it's important that we go through them.

**Hon. Tony Clement:** Sure, and let me say that if you look at clause 10, you have the definition of "express consent", including under subclause 10(4), and the definition of "existing business relationships". I would encourage the committee to go through that list. There's also, under subclause 10(6), the definition of "existing non-business relationship". So go through that list and find out whether that makes common sense to you.

I'm not going to opine anymore, because I'm going to get myself into trouble with Mr. Rota again. I'm guessing that part of his question is at least answered in subclause 10(4). But let's go through that and make sure it covers things in a common-sense way and meets our objectives.

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

**The Chair:** Thank you, Mr. Masse.

Mr. Lake, please go ahead.

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

I want to talk a little bit about charities and maybe companies that conduct research—those kinds of companies. Can you talk a little bit about how the protection would affect them—probably charities in particular—so they don't get lumped in with spammers?

**Ms. Helen McDonald:** Under subclause 10(6) it talks about donations or gifts and it talks about volunteer work. There's usually an 18-month period that allows that relationship, if you like, to continue. So that's one way in which what are called “existing non-business relationships” are protected.

I think you talked about political parties. There are also provisions in subclause 10(6) for members of associations or parties, clubs, voluntary associations. They also have an 18-month period—if you have a relationship with them—to allow these kinds of messages to be sent, because presumably it may be an annual event or something else that you might want to protect.

I think the other point we want to be clear about is whether it's commercial or non-commercial activity, to try to make sure we are looking only at those things that are commercial in nature. So that might rule out some types of relationships.

• (1745)

**Mr. Mike Lake:** Okay.

You talked a little bit about the international reputation Canada has, and it's not a very good one in regard to spam. Can you talk a little about how that affects—and I know the minister talked about this—our international cooperation? It's very difficult, if you're not meeting the standard, to get cooperation. How does the international cooperation piece of this legislation work?

**Ms. Helen McDonald:** It envisages the three separate organizations—the Privacy Commission, the Competition Bureau, and the CRTC—as being able to work with their counterparts. I wouldn't have described it quite as Interpol; I'd describe the communications regulator in Australia as the counterpart for the CRTC. It's the organization charged with oversight and implementation of their equivalent act. So our bill would allow the CRTC to share information with Australia to help Australia apply its own law if perhaps the spammer is located in Canada.

We can also work with them to try to make sure that spammers located in, say, some European countries, if they have a substantially equivalent law... It can't be Australia; it must be some other jurisdiction because Australia has dealt with most of them. It probably allows them to exchange information with us that would allow us to help go after spammers from other countries who are targeting Canadians. Unless you can share information, you can't really take action against them. The provision of the bill allows that

kind of provision of information and collaboration across these, essentially, administrative arms of government.

**Mr. Mike Lake:** I guess there would be no borders when it comes to this. Ultimately, the fact that we don't have legislation right now sort of contributes to this idea of Canada almost as a haven for spammers. They send from Canada to other countries where they have laws, but they can't touch the spammer in Canada. Is that—

**Ms. Helen McDonald:** And we can't help them. Not only can spammers stay in Canada and feel somewhat protected, because there are no laws in Canada that allow us to go after the spammer, but it also prevents us from sharing information that could be helpful to these other jurisdictions.

**Mr. Mike Lake:** Just changing direction a little bit, Mr. Garneau talked about sort of casting the wide net, and I think Mr. Rota kind of touched on it as well, almost in a negative way. I understand the concerns they're bringing up there, but I would think that in an area like this, where technology is changing all the time, the danger of not casting that wide net, in a sense, is that you're going to be changing your legislation every time technology changes, right?

**Hon. Tony Clement:** Yes. I was saying that rather inelegantly, but that's exactly my point.

**Mr. Mike Lake:** Okay. Thank you.

**The Chair:** Thank you, Mr. Lake.

Madam Coady.

**Ms. Siobhan Coady (St. John's South—Mount Pearl, Lib.):** Thank you very much, and thank you, Mr. Minister, Ms. McDonald, and Mr. Simpson, for being here, and so late in the evening. We really do appreciate it. It gives us a good overview of where your heads are with regard to this legislation.

First of all, I don't think there's a person in this room who wouldn't agree that spam is harmful and hurtful to industry and individuals and we have to do something about it, so I think you have our concurrence in that regard.

On this particular bill, there are some challenges that I think as the minister has indicated we do have to overcome. I guess my first question would be, did a draft of the bill go out to stakeholders, and did you get feedback from the draft?

**Hon. Tony Clement:** We did not do a pre-existing consultation on the draft itself. We announced, I guess around April 24, that the bill was there. But we'd had a lot of contact with stakeholders prior to that to get their sense of what was necessary.

**Ms. Siobhan Coady:** That dates back to, say, the anti-spam round table of 2005. I think looking at what the anti-spam round table of 2005 did, this bill goes beyond what the discussions were at that time. Ms. McDonald's point is that she's looking towards our investigations over the next number of weeks as critical to improvements to the bill, because there are improvements required. For example, there are the anti-spam provisions from Mr. Garneau. I'm going to talk a little bit further about that.

I'm concerned about the address-harvesting provisions. As I understand them, it does remove some of the widely accepted generally applicable exemptions under the legislation, for example. There are concerns about that. I'll get to those. There are concerns that the anti-spyware provisions are a bit broad. So there a number of issues that we're going to have to focus on. Mr. Garneau talked about the extraterritorial provisions, as well as some of the remedies.

Just let me get to the anti-spam, if you would be so kind, because the main anti-spam provisions are found, I think, in clause 6. You've clarified what they are. The spam task force network and technology working group in May of 2005 had a different interpretation, much more succinct. The bill assumes that all electronic communications of unwanted spam, and we've talked about this.... It prohibits all commercial electronic messages, except in very limited circumstances. That's where I believe, Mr. Minister, that you indicated that we'd probably see acceptable commercial activity outlined in the regulations. Is that where you're going to put most of these?

• (1750)

**Hon. Tony Clement:** Well, there are some found in the actual body—

**Ms. Siobhan Coady:** Some are found under clause 10.

**Hon. Tony Clement:** —but for others, obviously, we have a catch-all in paragraph 6(5)(c).

**Ms. Siobhan Coady:** Yes. But the bill's scope really does depart from the anti-spam legislation found in other areas or among our international counterparts. For example, if you look to the EU directive and the U.K. act, they talk about direct marketing. The Australian spam act and the New Zealand spam act really define it towards direct marketing. Singapore looks at direct marketing.

Did you consider narrowing the scope? When you look at what your scope is, it's very, very broad; it's a catch-all. We've talked a bit about that. Other legislation around the world is absolutely more defined to direct marketing.

Do you have any comments on that?

**Ms. Helen McDonald:** I can ask Richard to speak more directly about what we learned from other countries and their experiences, but I think we were concerned that if we narrowed it too much, people would claim they were not doing direct marketing, but something else—the provision of information, or something else. You want to make sure you capture the behaviours that are clogging our e-mails and discouraging people from moving online. So we tried to restrict it to focus on the unsolicited and commercial activities, with a series of exemptions—which I don't think are tiny—laid out to try to make sure the legitimate businesses could continue, while actually putting a stop to the behaviours and practices slowing down electronic commerce.

**Ms. Siobhan Coady:** Can I take up a couple of examples? This is why I'm concerned.

For example, if I'm a business and I'm going to send an e-message concerning a product recall or a warranty, for example, with safety or security information, and if I hadn't been in contact for more than 18 months, because it had been purchased more than 18 months previously, we would not be allowed, as I understand it, to do that because it would be considered spam. That's quite a concern to me,

because on a warranty or a product recall, it would be very, very important to be able to discuss that.

I have other examples.

Do you want to handle this?

**Mr. Richard Simpson:** Yes, thank you.

For the example you used of a warranty or some form of communication relevant to a product, there are two possibilities. First of all, there could have been express consent when someone bought the product that they always wanted to have information on warranties, or anything related to the safety of a product, or anything along those lines. But even if not, the implied consent in an existing business relationship would work in that situation. The 18-month time limit is just a way of trying to find some date certainty regarding when that business contact is stale. But that's a detail that can be looked at.

If I could go back, Mr. Chairman, to the question about the spam task force and the work that was done, I'm pretty familiar with the thinking of the group, having been involved in the working groups and the task force itself. It's interesting that people like Tom Copeland, president of the Canadian Association of Internet Providers—whom the minister mentioned earlier had expressed support for the legislation—was a member of the spam task force. Most of those members would see the bill as very much consistent with the framework they had put in place. However, there are aspects of the bill that you would see in the work of the spam task force that we need to develop, such as defining the practices that will be part of the regime of implied consent. The regulations the minister referred to are going to be used to pick up some of the details we need in order to make the bill work effectively in a business environment.

Specifically, in the spam task force report, there was a piece of work done by the Canadian Marketing Association—the president, John Gustavson, who was another member of the task force. The CMA has come out in support of the bill. The annex I'm talking about was a set of industry guidelines for commercial e-mail marketing.

Our intention has always been that those guidelines developed by the spam task force, and later adopted by the Canadian Marketing Association, and endorsed by a number of Canadian businesses, would be reflected in the regulations and therefore in the operating principles of Bill C-27 when it became law.

• (1755)

**The Chair:** Thank you, Mr. Simpson.

Thank you, Madame Coady.

[*Translation*]

Mr. Vincent, do you have any questions?

**Mr. Robert Vincent (Shefford, BQ):** Yes. I just have a quick question.

I am wondering about the problem we came up against around the end of last year or the beginning of this year having to do with the do not call list. It bothers me a bit. Some people have been able to purchase, via the Internet, the telephone numbers on the do not call list. Individuals on the list were contacted by telemarketers.

Given what happened, I understand what Mr. Clement was saying earlier, that is, there may be a similar list for email addresses, which would prevent certain people from sending spam. However, that list would definitely be available on the Internet. Thus, people from countries without spam legislation could buy the do not email list on the Internet, just as people did with the do not call list. Then they would be free to contact people on the list and send them spam and advertisements from abroad, from countries where they are not subject to any legislation.

I want to know how you plan to address that issue on the Internet. Here in Canada, people have been able to get a hold of the do not call list. If they can do it here, I would think that elsewhere in the world where such legislation does not exist, people could get the list by some other means to advertise on behalf of someone else.

**Hon. Tony Clement:** First of all, as I mentioned, it is of course impossible to have a bill that fully and completely protects Canadians from spam or other means of electronic communication. However, I think this bill is significant because it allows us to join the ranks of nations that address issues such as spam.

Helen, is there something else you want to add?

[*English*]

**Ms. Helen McDonald:** When we talk about the do-not-call list, it's an opt-out. You put your name onto a list to indicate you do not want to receive telemarketing calls. So there will not be an Internet list for opting out of spam. It's a different regime from opting in; there won't be a single list created of all Canadians who do not wish to get e-mail spam or unsolicited commercial text messages. So there's quite a difference between those two approaches.

On your point about the fact that there is a list and what would happen in other countries who might be able to see this list, I believe that happened at the beginning, but the CRTC is taking steps to try to prevent the purchase of the names on the do-not-call list.

● (1800)

**The Chair:** Thank you, Madame McDonald.

Thank you, Mr. Simpson.

And thank you, Minister Clement, for appearing in front of our committee to explain this bill. We appreciate it. Your testimony will be helpful.

This meeting is adjourned.

---







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

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

**Also available on the Parliament of Canada Web Site at the following address:  
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :  
<http://www.parl.gc.ca>**

---

**The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.**

**Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.**