House of Commons
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 029 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Tuesday, June 16, 2009

Chair

The Honourable Michael Chong

Standing Committee on Industry, Science and Technology

Tuesday, June 16, 2009

● (1530)

[*English*]

The Chair (Hon. Michael Chong (Wellington—Halton Hills, CPC)): Good afternoon. Welcome to the Standing Committee on Industry, Science and Technology and to our 29th meeting this 16th of June 2009.

We're here to study Bill C-27, pursuant to an order of reference of Friday, May 8, 2009.

In front of us today we have four entities. We have Mr. Wally Hill from the Canadian Marketing Association, Susanna Cluff-Clyburne and Mr. Barry Sookman from the Canadian Chamber of Commerce; Mr. Bernard Courtois from ITAC, the Information Technology Association of Canada; and Madam Suzanne Morin appearing as an individual.

We'll begin with opening statements of about five to seven minutes from each of our four organizations, beginning with the Canadian Marketing Association.

Mr. Wally Hill (Vice President, Public Affairs and Communications, Canadian Marketing Association): Thank you, Mr. Chairman.

On behalf of the Canadian Marketing Association, we're very pleased to appear before your committee to speak about CMA's view of Bill C-27, the proposed Electronic Commerce Protection Act. Joining me here today is the chairperson of our association's ethics and privacy committee, Madam Barbara Robins, who is also vice-president of legal and regulatory affairs for Canada, Asia-Pacific, and Latin America for *Reader's Digest*.

The Canadian Marketing Association is the largest marketing association in Canada, with 800 corporate members and subsidiaries, including the country's major financial institutions, insurance companies, publishers, retailers, charitable organizations, agencies, relationship marketers, and those involved in e-business and Internet marketing. The association has a code of ethics and standards of practice that is mandatory for our membership. It is a self-regulatory code that provides CMA members and other marketers with a comprehensive set of best practices, including those related to consent-based e-mail marketing. The CMA was pleased to be a significant contributor to the 2004 and 2005 task force on spam. While there have been many changes in both the economy and relevant technologies since the work of the task force, we're pleased to see that many of its recommendations are reflected in Bill C-27.

Electronic commerce in Canada has evolved rapidly, and it has grown to become a key marketing channel. Research conducted for CMA by Global Insight calculated that for 2007 the Internet as a marketing channel drove nearly $17 billion in sales revenue and supported some 75,000 jobs in Canada. The current economic climate notwithstanding, this is a channel that will continue to grow and is expected to become the dominant driver, with anticipated sales revenue to climb to nearly $46 billion by 2011.

The 2009 global consumer e-mail study issued by Epsilon confirms that e-mail is the primary online communications tool for 87% of North Americans and that it continues to grow as a means replacing traditional transactions. Unfortunately, people identify two-thirds of that e-mail as spam, and that view, along with more serious spam-related threats of fraud and identify theft, continues to undermine consumer confidence in the channel. At the same time, ethical businesses see their brands hijacked and online customer relationships jeopardized.

The CMA supports the Electronic Commerce Protection Act because we believe it will put in place a framework and enforcement regime to significantly reduce spam and go after malicious online activity while balancing that goal with the need to promote economic activity and allow responsible marketers to continue using the channel for consent-based electronic communication. We do have some comments and specific suggestions that we believe would make Bill C-27 a better piece of legislation.

First, CMA believes it is premature and unnecessary to include clauses 64 and 86, the provisions that would allow for the dismantling of the national do-not-call program. While the government correctly points out that technology convergence may at some point make this a sensible option, we believe that such proposed changes, along with an assessment of the program, should be brought back to Parliament for careful consideration at such a time. At this point, the only real measures of the program consist of a Harris/Decima survey conducted for the Marketing Research and Intelligence Association, which found that 80% of the nearly seven million Canadians who have registered for the service find that they are getting fewer calls.

We're also pleased to see the exemption in the bill for business-to-business commercial electronic messages that is set out in paragraph 6(5)(b). Although we do feel that the current language could prove to be more restrictive than intended, we understand that Parliament does not want to impede regular communications between businesses. To clarify this point, the committee could look at alternative language, perhaps that used in Alberta's Personal Information Protection Act, to exempt the business contact information. That language would accept all business-to-business electronic communication that—and this is a quote from the Alberta legislation—

> is for the purposes of contacting an individual in that individual's capacity as an employee or an official of an organization and for no other purpose.

● (1535)

We expect that other witnesses will offer more detailed assessments; however, we recognize there is a concern about the installation of the computer programs prohibition that's contained in clause 8, and that could adversely affect some commonly accepted and routine online interactions. These include software transfers to facilitate program updates and to identify browser preferences so as to enhance users' online experiences.

We believe the committee needs to carefully examine these provisions with the input of expert witnesses, with an eye to providing greater clarity as to the impact.

CMA supports the notion that the ECPA requires adequate penalties as part of an effective enforcement regime. However, we are concerned that the multi-million-dollar administrative monetary penalties proposed in the bill are excessive, given that they are not subject to the same rules of evidence and due process of civil and criminal proceedings. So we would ask that the committee consider the potential chilling effect this could have on law-abiding companies engaged in commercial electronic communications.

I point out to the committee that when the national do-not-call program was put in place, the penalties in that act were up to $1,500 for individuals and up to $15,000 for companies, for each transgression. The penalties in Bill C-27 are considerably larger than that.

We recognize that the ECPA takes a different approach than the CAN-SPAM Act in the United States, but we have a couple of suggestions to improve consistency between the two laws. Specifically, we suggest that the required contents of a message be changed to specify that only the identity of the sender need be included in the message. We also suggest that the timeframe for executing unsubscribed requests should be clarified as being 10 working days. In the act currently, it is 10 days, and making that small change would put marketers who are engaged in marketing campaigns across both countries on the same page in terms of the legal requirements.

Finally, we take this opportunity to ask for the committee's support in urging the government to commit to a thorough public communications program when the law goes into effect. We ask that the government adopt a pre-implementation program and timetable that will promote business preparedness for the new framework. This will help to build compliance, while at the same time reducing consumer complaints.

Barbara, do you have anything to add?

[*Translation*]

Ms. Barbara Robins (Vice-President, Legal and Regulatory Affairs, Reader's Digest, Canadian Marketing Association): I would like to echo the comments of Mr. Hill on behalf of all of the members, entities and businesses that serve on our association's ethics and privacy committee.

Consider, for example, Reader's Digest which has been publishing in Canada for at least 70 years. Our company wants and must adapt to new technologies such as the Internet, the Web, and so forth. It is very important to Reader's Digest and to other business members of the association that their legitimate businesses activities not be confused with those of businesses that send out electronic business messages without consent. That is the first reason why we support this bill.

Secondly, we support the bill because it calls for a very reasonable and balanced approach to be taken. The proposed section 13 stipulates that the burden of proving that consent has been obtained, pursuant to sections 6, 7 and so on, falls to businesses. However, the bill is drafted fairly and allows businesses enough flexibility to decide on the required approach to securing consent.

Thirdly, the bill is consistent with many other laws in place in countries around the world. For instance, Australia, New Zealand and Singapore have had legislation that adopts a similar approach in place for several years. For Canadian businesses that operate on an international scale, it is important to have a more or less harmonized approach. However, Canada must retain its reputation of having very solid legislation. This is not considered a lightweight piece of legislation.

● (1540)

The Chair: Thank you, Ms. Robins.

[*English*]

We'll now hear from the Canadian Chamber of Commerce.

Mrs. Susanna Cluff-Clyburne (Director, Parliamentary Affairs, Canadian Chamber of Commerce): Thank you, Mr. Chair.

I send apologies on behalf of Shirley-Ann George, our senior vice-president of policy, who is ill today.

Appearing with me today is Barry Sookman, who is with McCarthy Tétrault. Barry is widely known as an expert in Canadian technology law. He is the author of the leading Canadian five-volume treatise on computer and Internet law and is an adjunct professor at Osgoode Hall in Toronto.

It is a pleasure to be able to present the views of the Canadian Chamber of Commerce and our members on Bill C-27. As many of you know, the Canadian Chamber is the largest business organization in Canada, with membership of 175,000 businesses in all parts of Canada. Our members include both the largest and the smallest of companies. We pride ourselves on being the voice of Canadian business and work hard with politicians and government officials to ensure that Canada's business community is able to maximize its economic and social contribution to our national well-being.

Let me start by saying that the Canadian Chamber strongly supports the goal of eradicating spam. We also participated in the 2005 spam task force, and at our 2007 annual general meeting, the Canadian Chamber and our members from coast to coast to coast passed a policy resolution calling for measures to curb spam. Today, Canadians and Canadian businesses of all sizes and from all regions need effective legislation to limit the scourge of spam. At the same time, Canadian business does not need to be burdened by overly broad legislation that restricts legitimate business activities. To net it out, we need to deal with the bad guys that waste countless and costly hours in every business in Canada and use the Internet to distribute mass mailers that prey on the vulnerable.

Bill C-27 is still a work in progress, and we are here today to call for much-needed modification. This bill, as currently drafted, may render thousands of commonly used computer applications illegal. It would submit Canadian businesses to potential fines of up to $10 million. This new Electronic Commerce Protection Act would also amend the Personal Information Protection and Electronic Documents Act, PIPEDA, to submit Canadian businesses to civil suits resulting from violations of the act. This bill would also effectively 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.

We appreciate the government's efforts to introduce and pass a bill that will help stop spam. Unfortunately, this bill needs to be fixed. We urge members of this committee to take their time with this 77-page bill, so that government can bring to you the necessary repairs, and so you can pass a bill in the fall that we can all agree on, one that will be effective in stopping spam while not inhibiting legitimate business practices.

I will now turn it over to Barry to discuss the specifics.

● (1545)

Mr. Barry Sookman (Partner, McCarthy Tetrault LLP, Canadian Chamber of Commerce): Thank you, Susanna. Thank you, Mr. Chair.

I would like to reiterate the importance of legislation to deal with problems being tackled by Bill C-27. I think everyone agrees with the basic objectives of the bill. Some of the features of the bill, however, could create inadvertent problems. I will focus on these problems, but my comments should not be taken as a lack of support for the bill.

At a high level, there are two main problems with the bill. First, the bill does not adequately balance the objective of preventing unwanted or harmful behaviour with the objective of ensuring that perfectly legitimate acts are not made illegal and the goal of preserving the vitality of the Internet for electronic commerce. Second, it introduces conflicting or unnecessary regulatory regimes that needlessly impose significant costs on business.

The scope of the anti-spam provisions are very broad. The ECPA applies to all electronic messages, including messages that are business to consumer, business to business, consumer to consumer, and consumer to business, subject to very limited exceptions. To be caught, messages must simply have as a purpose to encourage participation in a commercial activity. The limitations on the constitutionally protected right to commercial speech are far broader than legislation passed by other governments. Its open-ended net could result in making perfectly desirable communications illegal.

Australia and other countries also use the term “commercial electronic message”, but they confine its application to a defined list of business-to-business and business-to-consumer messages that offer to supply, advertise, or promote a product and service essentially to direct marketing.

It has been argued that we shouldn't worry about the scope because there are exceptions that cover all legitimate communications. I almost missed the business-to-business exception when I first read it because it was so narrow. It applies only to sending a message that consists of an inquiry or application. It doesn't permit a range of messages that can be sent to a business, including sending e-mails to a potential new partner, distributor, or supplier about potential new business, even if their contact details are published on the Internet, or sending out e-mails to a contact list developed over a lifetime when starting a new business or changing jobs would also be prohibited. Even including an e-mail invitation to go for a coffee or lunch to talk about business could be banned, unless you've entered into a contract with that person in the last 18 months. The bill would literally also prohibit consumers from e-mailing retailers, demanding a refund, asking for support, or making a warranty claim within 18 months after purchasing a product.

The examples illustrate the problems associated with the so-called features of the bill. Regulations to expand exceptions will never keep pace. It is far easier to use regulations to close loopholes spammers may devise than it is to keep pace with the indefinable and potentially unlimited range of messages that may be communicated among Canadians. There are also significant potential problems with the personal or family exception.

You have also been told not to worry about the broad prohibitions in the bill because consents are implied in many situations, but under the bill, implied consent exists only where the sender has an existing, narrowly defined business or non-business relationship. That definition does not catch the diversity of actual business relationships that entities may have. The consent provisions are much narrower than in other jurisdictions, such as Australia and New Zealand. These countries accept that consent can be expressed or implied from the conduct of a business and other relationship, or inferred from a conspicuous publication of an electronic address on a website.

PIPEDA, our privacy legislation, permits consent where it may be inferred from the action or inaction of the individual. This standard was agreed to by all stakeholders as part of the CSA model code in PIPEDA, so the impact of the ECPA's higher standard would be that legitimate Canadian businesses would now be subject to conflicting standards. They would have to revisit all of their practices, and this is especially of concern to the chamber members.

● (1550)

The extraterritorial effect of the bill is problematic for Canadian companies.

The address harvesting provisions are not tied to the collection of information for the purpose of using it to send spam, as it is in other countries.

The bill would render inapplicable all of the general exceptions in PIPEDA that are used to collect, use, or disclose personal information. This would include exceptions for private and public law enforcement or to comply with subpoenas, warrants, or orders made by courts. It could be very significant for private and public law enforcement in Canada.

There is also no exception covering network service providers caught by these provisions.

The anti-spyware provisions make it illegal for a business to install any computer program on somebody's computer without consent. The prohibition is not limited to “malware”.

The spyware provisions would establish a whole new and unnecessary regulatory regime covering the installation of beneficial computer programs. No one has studied the costs and technical difficulties of complying with these new rules with the myriad of digital devices that exist today and that will be used in the future.

I would like to thank the committee for the opportunity to speak today. I look forward to answering any questions you may have and working with you towards getting a stronger and better bill as soon as possible.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Sookman.

We'll now hear from the Information Technology Association of Canada.

[*Translation*]

Mr. Bernard Courtois (President and Chief Executive Officer, Information Technology Association of Canada): *Merci, monsieur le président.*

Mr. Chair, I am delighted to be here this afternoon to voice our support, as a business association, for this anti-spam legislation.

I'd like to begin by telling you about our association. We are well known, but it might be a good idea to remind you that

[*English*]

the companies that make up our membership—we're the national association of the information and communications technology industry—make the hardware, make the software, offer the services, and create the applications that make the Internet, make it work, and help people use it. Our members are very heavily involved in fighting spam and fighting malware and in helping Canadians to fight these. They deploy tremendous efforts to do this, and we believe that legislation will help in that fight. We therefore support the bill, and we support going after spam—spam against consumers and spam against businesses as well.

I was also personally a member of the spam task force, and I recall that we had a lot of discussions around the concept of spam and the fundamental approach to the issue. All the members of the task force, whether consumer representatives or business representatives, agreed to an opt-in regime, which, by the way, was not the rule in the U.S., and we thought there were flaws there. We also agreed that legislation should cover more than spam and address other topics such as spyware and malware, but I have to say we did not have as much discussion there about what particular approach to take. We definitely wanted to have something that would go after spyware, but we hadn't resolved how to do that without impeding a lot of the legitimate transactions that take place.

We are here to offer our expertise to the committee, and we're offering to bring our expertise and work with the government to handle the changes we need to make to the bill to make sure it doesn't have unintended consequences. The whole purpose of this legislation is to facilitate and increase confidence in the use of the Internet and the digital economy by Canadian businesses and consumers. We approach the changes that we need to make to the bill so that they actually achieve that purpose, as opposed to possibly impeding electronic commerce and making it in some cases more difficult to protect consumers. For example, as Barry has indicated, there are some practical, day-to-day things that everybody would say absolutely need to be able to continue, and they should not be made illegal under the bill.

I see two categories here. When we're talking about spam itself and areas such as implied consent or inferring consent from the circumstances, I think all of us can look to a specific list of practical day-to-day examples and say let's work on the language of the legislation so it does not cover that.

Then there are more technical aspects to the bill. When we come to spyware and malware, or redirecting ISP addresses, or harvesting ISP addresses as well, we fall into a world where even the lawyers who have been involved in this area for many years need to go to our technical people and say let's think through how things work, and ask for some examples of how things happen on the Internet to help users or consumers. We don't realize how it works, and until we do, we may not be able to get the right language in the bill to make sure we don't capture things we don't like.

All our computers need to be protected against malware almost instantaneously when we turn them on, for example. Every second the computer is on the Internet and not protected leaves it open to being infested with viruses that are very difficult to deal with.

Just to give you an example, if you put in a system that has to have the consumer approve a very urgent patch to a gap in security on the computer, the consumer might click on that right away or they might go and get a coffee while the computer is getting turned up, and then you go a few minutes with the thing unprotected. So you don't want that.

You also want certain interventions to be done without really representing a significant transaction. There may be things that happen very automatically, very quickly, and you don't want to start impeding that by requiring explicit consent.

● (1555)

It might be difficult to describe that in sufficient terms, broadly enough, up front, to get the kind of consent you need. It's the same with the redirection of addresses. Sometimes it could be more than just an ISP or a service provider who furnishes the access to the Internet. It can be a site or a service provider that provides you with a portal or services. It could be a search engine and so on. Sometimes you type in a name wrong and the service will redirect you to the correct address you really wanted, and sometimes they will remind you, “Did you really want to spell it this way?” Those are all things that happen instantaneously and very smoothly on the Internet. We don't want to start making that very complicated.

For us, therefore, as I say, we need to work with our technical people to say let's think through all these things and then we can make the changes that are required.

I want to finish by saying that we support getting this bill through and we do not want any undue delay in it. I would say that's the basic theme that I find when I talk to the other business associations. We explain sometimes, by referring to principles or whatever, what we see are problems with the bill, but from our standpoint, the changes that are needed are doable. They're not changes in the principles of the bill. They fit the principles of the bill, and we suggest we approach them from a practical standpoint. You will find that we can make the changes that are needed to have the bill actually achieve its purpose, which is to facilitate electronic commerce and facilitate the use of the Internet by Canadians.

Thank you.

[*Translation*]

The Chair: Thank you, Mr. Courtois.

Go ahead, Mrs. Morin.

Mrs. Suzanne Morin (As an Individual): Thank you.

My name is Suzanne Morin and I work for Bell Canada.

[*English*]

I am assistant general counsel at Bell Canada, as well as Bell's privacy ombudsman. However, I am here today in an individual capacity.

You might wonder why. Bell Canada is a member of all the associations appearing here; however, I participated on the task force as an individual and I just thought it might be useful for me to share with you, in my own personal capacity, some of those experiences, but also why, as an actual representative from an organization, I was on the task force.

Since the early 2000s, we've been doing some work internationally with our counterparts as well as with governments on the Internet Law and Policy Forum, as well as on the Global Business Dialogue on Electronic Commerce, where we really initiated some of the beginnings, if you like, of the international discussion around spam and what to do about it. As you've heard today, no one can really define what spam is because it's all a matter of someone's perspective, but everybody agrees that there is definitely a whole bunch of e-mail out there, the millions and billions of e-mails you hear about that clog up our networks and fill up the inboxes of users.

Through a lot of that international discussion, where players ended up was determining that there were two buckets, if you like, of unsolicited e-mails. There was that bucket that was truly harmful, where this wasn't about seeking consent to use someone's e-mail; this was about using false headers and false reply addresses, and it included selling false goods. There was this notion of falsity and fraud incorporated in them.

Then there was this other bucket, becoming smaller and smaller as the years progressed, because as you've heard, unsolicited commercial e-mail represents about 90% of e-mail circulating on the Internet today. So this smaller bucket was more in the sense of fair practices and whether or not organizations were actually adopting those. For example, the real estate agent scenario that we've heard about over the last week is not the kind of situation that internationally we thought actually made sense to go after, because typically privacy legislation would deal with those kinds of scenarios. So that , because we have privacy legislation here in Canada, and it would be perfectly normal that the complaint would be dealt with through that complaint process, through a kind of one-on-one, and usually the Privacy Commissioner would try to mediate that away. So we have existing privacy legislation in Canada—if we come ahead a few years now—that can deal with a lot of the scenarios and a lot of the unintended consequences potentially than what ECPA does.

However, ECPA definitely has a lot of the tools that in fact are needed to go after the really bad actors, those 17 bad spammers who still live and operate in Canada. A lot of different organizations can tell you, “We know who they are, we know where they live, and we know how they operate. We just need the tools in order to be able to go after them easily.”

If you compare that, however, with some of the statements you heard just a few moments ago, the issue is how do you balance a new regulatory regime to go after these bad actors while not imposing on legitimate Canadian businesses, who are really subject to privacy legislation and consumer protection legislation? And there are definitely different approaches to legislation.

I support privacy legislation, but how do we ensure that balance, given the framework that's been adopted? I think what you've heard here is that a lot of people have spent a lot of time thinking about these issues, and this is a very complicated piece of legislation. Every day that we speak with Industry Canada, either at a hearing here or over the phone, we better understand the intent behind some of the provisions that were there. But we don't fully understand the potential consequences it might have and how it might actually play out.

So I think what you've heard is that additional time is needed to work with Industry Canada. They've gone through a lot of effort to try to deal with some of those unintended consequences to try to make sure that legitimate businesses aren't hampered. But those are in fact good intentions, and words on a page are interpreted by courts and by regulators, and we don't know who will be interpreting those words. Just like that real estate agent example, he or she shouldn't have to file an undertaking with the CRTC if they make a mistake. They should be dealt with before the Privacy Commissioner's office through a very simple complaint and that would go away.

The last thing I might mention, in closing—because the dialogue that might happen is what we are really looking forward to—is that I actually filed a second spam complaint with the Office of the Privacy Commissioner, along with Professor Michael Geist. PIPEDA, our privacy legislation, proved to be perfectly capable of dealing with that situation. This was someone who owned pontoons on the east coast and wanted to sell them. He engaged a third party to send out e-mails to professionals. I happen to be a lawyer, so I was on a list of lawyers he got access to. It was as simple as that. I just happened to be on the task force at the time, and I thought this was perfect: a Canadian selling Canadian goods in Canada. Do we have legislation that can deal with this? Sure enough, PIPEDA rose to the challenge. The person changed his practices. His e-mail marketer changed their practices, and that was great. He wasn't subject to having to sign undertakings. He wasn't subject to significant AMPs.

● (1600)

The last point is a little bit of a discussion, and Mr. Hill referred to it as well. Is legitimate business being faced with significant monetary penalties, whether they're from a regulator or through private right of action? There is a lot of expense for organizations to ensure that they do their due diligence and change their practices so they aren't subject to those types of suits, whether it's before a regulator or before the court. Again it's the notion of balance. How do you go after the bad guys without unintentionally overburdening legitimate business?

With that, I welcome your questions.

● (1605)

The Chair: Thank you Madam Morin.

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

Mr. Anthony Rota (Nipissing—Timiskaming, Lib.): Thank you, Mr. Chair.

Thank you to our guests for being here with us today.

Two areas that concern me about this legislation are the breadth of it and some of the remedies that are being proposed. This committee has been confronted with two different models for legislation dealing with spam and spyware. On the one hand, it's argued that a feature of the legislation is its breadth. It's argued that expansive legislation is needed to protect against changing tactics used by spammers and those who would introduce malware into our computers. It's further argued that problems with overbreadth can be handled through regulation. On the other hand, we hear that the broad sweep of the legislation could be a problem, and a preferred approach is a more narrowly focused and targeted law.

Do you believe that a more targeted approach is preferable? Would that approach leave Canadians vulnerable to new techniques used by spammers and distributors of spyware? How do you achieve a balance, and how do you decide which approach to take when dealing with an issue like this?

Mr. Bernard Courtois: I'm not sure that one approach is the right one for all the elements of the bill. For example, when it comes to spam, you could either narrow the definition of spam and make sure you catch all the bad behaviour, or you could take a broader definition of spam but work quite a bit on inferred consent and implied consent.

With spyware, you could either create a longer list of things you think are good—software downloads and update patches—and make sure all those exceptions are covered and the regulations can add more, or you could just put in the definitions of the elements of spyware.

In the case of spam, it might work better to look at implied consent and legislation that's been used in other countries that we know works in practice. We could take the best of that and make sure we go through the practical examples and say, “Okay, if we write it this way, then these good examples will not get picked up.” So those are the pros and cons there.

I think everybody would agree pretty quickly on the list of five or six things that constitute malware—the bad things in spyware. You can say in the regulations that we can add to that if the bad guys think of new ways we haven't thought of to date. I think there would be very few examples of that happening. If you try to do the reverse and define all the good things that take place that shouldn't be captured by your anti-spyware provision, we'll have a much harder time exploring that total universe. You have very different types of transactions that take place.

I think the pros and cons weigh in favour of defining upfront the bad things you're going after and allowing additions to that, rather than trying to define upfront exceptions that wind up being longer and longer. You're going to fear that you haven't caught certain circumstances, and someone might find themselves subject to massive administrative monetary penalties or private lawsuits while you think through the legislative changes or the regulatory changes, because regulations don't get changed in 24 hours.

Mr. Anthony Rota: Would it be fair to say that the legislation we're looking at now is a little too broad and needs to be narrowed down? I think that's what I'm hearing.

Mr. Bernard Courtois: Yes. That's why I'm saying that these are very specific changes that need to be made. When you define the spyware provision, you can then put the specific items. That's not a big change to the legislation. It doesn't affect the principle. In the case of spam, you can define those implied consent things.

When we say yes, it's a little too broad, it doesn't mean that bill needs wholesale change. It means you look at very specific sections and say that we can add some language that narrows it either in the upfront definition or by setting out more or broader exceptions.

● (1610)

The Chair: I think Mr. Sookman had something to add.

Go ahead, Mr. Sookman.

Mr. Barry Sookman: Yes. Thank you.

If I could supplement that, I agree with a lot of what Bernard was saying. The international experience is really helpful on this, because many countries have gone before us in enacting this kind of legislation. There is now a fair consensus that Australia is a good model for this. Their legislation was followed by legislation in New Zealand, Hong Kong, and Singapore, so it does have some lessons in it. Their approach, which has been proved to be effective, as this committee has heard, was to target very specific acts and to have generally applicable exceptions. That approach has worked very effectively.

In the Internet context in particular, it is such a dynamic medium, with new technologies and means of communications being used all the time. The prospect of banning potentially legitimate behaviour and thinking that regulators could keep up with all the new forms of communication, and that new forms of communication would become legal as regulations were passed, I think would be an approach that would be exceptionally enormous. It would put Canadian businesses potentially behind our international counterparts, which wouldn't be living with those kinds of prohibitions.

Mr. Anthony Rota: What I'm getting, then, is that what we want to avoid is a wide net that's going to bog down the system and where nobody will want to use it because they're afraid of being charged with some kind of crime.

If I can go to the remedy part, I want to ask you about a scope of remedies in the bill. We're told that the stern remedies are needed to deter spammers and purveyors of spyware. We're also told that some Canadian businesses are concerned about the potential for class actions, especially given the potential for statutory damages that could be as high as $1 million per day. We've also been told not to worry about the class action system because the Canadian system is different from the U.S. system.

Are there any changes needed to the penalties or to the private right of action portion of this bill? What concerns me, I guess, is that Mrs. Morin mentioned the real estate agent who does not make $1 million a year—or whatever fine it would be—and suddenly finds himself or herself charged in a situation where they were just trying to follow up on a lead and ended up with this large fine.

I guess it's not so much the fine that bothers me. It's that they have to go to a lawyer and suddenly are confronted with legal fees. Whether it's a real estate agent or an average person, having to fight a civil suit opens a whole Pandora's box. That concerns me. Should it be civil or should it be done through a regulator within the government?

I have a bunch of questions there, so I'll let you go on until we run out of time.

Mrs. Suzanne Morin: I'll just give you some thoughts. These are things that colleagues or other businesses have raised as well.

There are different ways to ensure that you have the sufficient AMPs; there is no doubt that the fines must be high. They must be significant or else they will just be viewed as a cost of doing business. There is no doubt that the $10 million is great to see, but who is going to apply to? There are different ways to ensure that the exposure to those kinds of penalties isn't faced by legitimate businesses. One of them is a narrower bill.

Another one is linking up, for example, unsolicited commercial e-mail with some of these other bad activities, so it's only if you send unsolicited commercial e-mail along with falsifying headers, or use inaccurate URLs where people go to visit, or accompany that with false information in the contents. You link it back to what is really the fraudulent behaviour, which is not just the sending of the e-mail; it's that business is trying to happen and I'm trying to obtain your personal banking information. If you link them to that and the AMPs are maybe attached more to those types of communications, that in and of itself already takes a lot off the table and definitely allows you to go after those 17 or 20 spammers here.

There are many different ways to do it, but the concept is to try to differentiate the exposure of the bad actors from legitimate Canadian business.

● (1615)

Mr. Anthony Rota: Zero in on intent rather than the action itself. Does that make sense? Is that a good way of describing it?

Mrs. Suzanne Morin: Or take a look at all the different elements that happen in these communications. As I said, the spammers today don't just send e-mails for the fun it. They're trying to sell you something, they're trying to get your personal information, they're trying to circumvent our spam filters. There's always something else fraudulent that they're trying to do. Maybe you'll link into that kind of an activity as well that's already included in that file. It's just a thought.

Mr. Anthony Rota: Thank you.

The Chair: Thank you very much.

Monsieur Bouchard.

[*Translation*]

Mr. Robert Bouchard (Chicoutimi—Le Fjord, BQ): Thank you, Mr. Chair. I would also like to thank each and every witness for their testimony.

My first question is for Mr. Hill, the Vice President of the Canadian Marketing Association.

You have proposed a number of changes or amendments. You have even suggested that certain clauses of the bill be amended. You also talked about the spam that circulates between the United States and Canada. Which brings me to this question: are you at all concerned about spam originating from country's other than Canada?

In Canada, Bill C-27 sets out the rules which allow for a certain amount of control. At the very least, it provides for measures that are applied within Canada. However, have you looked at what is happening outside Canada? If so, have you any recommendations to make on ways of curbing, eliminating or reducing spam originating from outside Canada?

A considerable amount of spam is indeed generated outside of Canada.

[*English*]

Mr. Wally Hill: Yes, spam is an international problem. I believe that part of what this bill intends to do is put in place the enforcement capacities and potential for international cooperation that will allow countries to collaborate and go after spammers in a variety of locations. The bill makes it illegal to send an unauthorized, without consent, commercial e-mail message to someone in Canada. That would equally apply to an organization that may be engaged in spam outside of Canada, but obviously, for enforcement purposes, our authorities will need to collaborate. And that's an issue that we find in a lot of areas.

What I was speaking about was the fact that we're operating in a North American marketplace. Much of our trade goes on between Canada and the United States, and they also have an anti-spam regime, somewhat different from this. I believe this bill will raise the bar on fighting spam here in Canada. But I was just looking for, and putting on the table actually, some suggested areas where we can achieve commonality between the two laws, without reducing the effectiveness of what's been proposed here in Canada, but by avoiding ethical businesses that are engaging in e-mail marketing campaigns in Canada and the U.S.

Many of our members have operations on both sides of the border. Try to get the requirements in e-mail messages, for example, standardized between Canada and the United States. There's a requirement in this bill for the identification of the sender of an e-mail, but added in the Canadian bill is the fact that any service provider that may have sent the message as well has to be included. Well, that's not included in the U.S. framework. For marketers who are operating on both sides of the border, it can often be difficult to tell whether a gmail.com account is in Canada or the United States. It's very difficult.

Businesses could find themselves inadvertently breaking the rules in Canada if we don't try to achieve some commonality between the two regimes, which is something we tried to do under the do-not-call list. You'll recall that the 18-month definition, which is actually in this bill, was initially discussed under that piece of legislation, and we were trying to find some compatibility with the telemarketing rules in the United States.

● (1620)

[*Translation*]

Mr. Robert Bouchard: Thank you.

My second question is for the Canadian Chamber of Commerce representative.

Judging from your comments, you are rather critical of Bill C-27. You alluded to the thousands of spam messages that would be considered illegal and to the prohibition of business relationships. You say that the bill needs to be improved.

What provisions of the bill do you find acceptable? Are there sections of the bill that you would be prepared to defend and that you would like us to go forward with?

[*English*]

Mr. Barry Sookman: As we mentioned in our remarks, we are very supportive of the bill in principle. We're also very supportive of the objective of dealing with spam and harmful or malicious computer programs that could have detrimental effects. We agree with the approach of opting in as opposed to opting out in the United States. As Mr. Courtois said, the issue is really recalibrating it to remove the inadvertent potential problems. There are several ways in which that can be dealt with. Some people will have different views on the best way to do this, because although there are certain common elements internationally, there are still variations from country to country. There needs to be discussion and debate on the appropriate approach for Canada to do this right.

As a matter of general principle in talking about spam, if the definition of the electronic commercial message were targeted at the real subject matter that's of concern to the country—these direct marketing types of messages that are the focus internationally—that scope would get the 17 bad companies that everybody's concerned about and not inadvertently catch the Canadian businesses that are just trying to hang on in these tough economic times.

On consent, if we move from express consent to the international standard of further implied consent, there is no way the 17 bad apples could ever prove they had implied consent. We would be able to catch the entities we're really concerned about without inadvertently catching legitimate Canadian businesses.

On the exceptions, if we didn't try to be very specific and identify every exception in advance, but left it to a flexible and realistic principle, we'd be far advanced.

On spyware, many countries simply rely on their criminal code provisions to deal with it. Canada has several provisions that would be applicable today, such as mischief in relation to data, and the unauthorized use of a computer. So there isn't necessarily a case that we need it. But if we were going to do it there are models in other states, particularly the United States, that have spyware legislation. They deal specifically with malware and define what it is. If we moved in that direction we would have a bill that everyone around the table would accept in principle.

● (1625)

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

[*Translation*]

Thank you, Mr. Bouchard.

[*English*]

Mr. Lake.

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

Thank you to the witnesses for coming today.

I'm interested in some of the terminology that's been used here. I hear a lot about "legitimate businesses", but really no definition has been given for that. I'd like to hear a little bit about that.

Also, the 17 bad guys—apparently there are only 17 bad guys out there.

Back at the last meeting, I talked about my days in the mid to late 1990s working at the Edmonton Oilers hockey club and having an e-mail address that I had to actually change eventually because I got so much junk. I tell you, that junk wasn't coming from these 17 bad guys you're talking about. It was junk. It was simply virtual junk that clogged up my e-mail so badly that I actually couldn't function properly using the e-mail system I had. I don't believe most of it was fraudulent e-mail; it was just pure junk. We had to hire an extra person to deal with it, we had to install software to deal with it, it took up tons of our computer space, and it eventually caused me to change my e-mail address.

I'm finding it interesting to hear—and I may be wrong, Mr. Sookman—but it sounds like you're defining that as legitimate business.

And Ms. Morin, although I see you shaking your head, it sounds like that's something you wouldn't want to see covered under this legislation. I just want to get some clarification, maybe first from you, Ms. Morin. Do you not see that as a problem? Should we be addressing that through this type of legislation?

Mrs. Suzanne Morin: No, actually a lot of the unsolicited commercial e-mail that you were probably getting in your inbox really would have fallen into the category of truly unsolicited messages, as they would have been using some kind of dictionary tag or software to harvest your e-mail address on the Internet. They're using another element where they're clearly not even trying to rely on implied consent or any other form. They're using methods to collect these e-mail addresses, and then they go off to any other vendor who's willing to sell their wares and they will send the e-mails for you.

I would still see most of that, actually, as something that should be caught by ICPA, and is caught by ICPA. I know "legitimate business" may be difficult to explain, but legitimate businesses in Canada are subject to privacy legislation, and it's proven to be useful, because these individuals that both Professor Geist and I referred to hadn't sent one or two e-mails; they had actually sent out hundreds of e-mails on their lists, and they just happened to hit two people who were on the task force, so it was their bad day.

Mr. Mike Lake: So it's fair to say we're not talking just about 17 bad guys, but an infinite number of really irritating guys.

Mrs. Suzanne Morin: There would be more than 17.

Mr. Barry Sookman: Thank you.

It's true, we all get irritating e-mails. Some of them we even get from people we like, with whom we have a personal and family relationship. So there's nothing we're going to do here to avoid getting e-mails that we don't all want to get. The issue is how you properly distinguish between the good ones and the bad ones, and that's where the debate is. I don't have any disagreement with you that all of those e-mails that clog up our e-mail inboxes from people we don't know and have never dealt with are ones that should be covered, and they'd be covered both by PIPEDA and by the ECPA. And they'd be covered even with the kinds of suggestions we were making to recalibrate the bill. Those e-mails that are clogging up our inboxes from people we don't know, they would not fall within the definition of implied consent or from a relationship we had. So I think we could deal with your clogged mailboxes—and they're all clogged mailboxes—even with a more flexible implied consent regime.

Mr. Mike Lake: I'll go to Mr. Courtois now.

In terms of Java and JavaScript, there have been some comments. The minister has been pretty clear that he's willing to take a look at some tweaking of the language to make that work.

I just want to talk about the general updates conversation. It seems as though, in my experience, when I put something on my computer, I typically get something that asks if I agree to the conditions, or whatever the case is. It doesn't seem like it would be all that difficult for the supplier of the software that I'm putting on my computer, whoever that may be, to just include a message that asks me for my consent when they want to put updates on my computer, regularly. I think, generally, if I'm putting on a piece of software to facilitate security on my computer, I'm going to be very happy to accept the suggestion that I might periodically get updates to make sure that software is updated.

Is that not enough? What would you suggest might be unreasonable? Would you suggest there's anything unreasonable about that expectation?

● (1630)

Mr. Bernard Courtois: I think that best practices can be reflected in the legislation. If I, for example, have downloaded a program that enables me to open certain applications or see videos or hear sounds, that's what I see now. When there's an update ready, I am asked if I want that update. The best practices are that while the updates are being downloaded, I just reduce them to the bottom of the screen, and I can go on using the computer.

It's very different when you're talking about some security patches or applications that really have to be downloaded automatically. That also includes certain types of transactions during which it's not quite clear that there's an actual program being downloaded. That's where I say we have to talk to our technical people and ask how many transactions like that don't really represent the format of "Do you want an update to this particular program you've installed? Click yes." And you know exactly what it's for. For some of them, if they are trying to fix some vulnerabilities in your computer, there's a timing factor and a complexity. There's a question of explaining what they're for, whereas conversely if you want to go after malware, you can write down the five or six things that constitute malware. They include modifying settings of other programs, collecting personal or financial information of the computer's owner, activating keystroke logging software to collect personal information, attempting to block or uninstall existing anti-spyware, collecting browser history and bookmark list, or preventing the user from removing spyware programs.

You could run down the list and make them subparagraphs in the definition of spyware, and you would get pretty much universal agreement to them. By regulation, any other similar thing could be equally prohibited, and you've covered the universe. You're trying to cover the universe of downloads, but what's the downloading of an applet or JavaScript? Is that a program? Does that lend itself to approval or requesting approval? Does it make the functioning of the Internet a lot more cumbersome?

That's where you really would have to get a group of people around the table, and you would never be totally comfortable that you'd covered all the cases of things that are good that you don't want to prohibit. That's why it's so easy to write down the bad things. Just list them and you've done what you've tried to achieve.

Mr. Mike Lake: What I'm not clear on is the instance of someone trying to access my computer from outside to fix some undefined problem, but something that would be urgent and crucial to fix. I'm not sure I understand. I can't think of an example. Maybe you can give me one of a situation in which the organization that's accessing my computer from the outside wouldn't have had an opportunity to get my consent in the first place. That's what I'm not clear on.

I get the fact that if I'm surfing the web, there might be some issues with things that might automatically be a part of my web experience that I don't want to stop from happening. I don't want to click on "OK" every time they happen. I get that part. Maybe there needs to be a tweaking to deal with that. I'm talking about this critical situation that you're talking about, that someone from the outside knows about and can solve. Give me an example of where they wouldn't have my consent.

Mr. Bernard Courtois: I have to admit that I'm not expert enough to know that, but I know that if the kinds of attacks and the kinds of problems that can occur were predictable, then obviously all the software would do it. You might want to be doing something to the program other than to say broadly up front that we can put in any updates that help better protect your computer.

Is that going to fit the definition of what we have here in terms of what the consent complies with? Are there other cases where you're downloading things that wouldn't necessarily be seen as a particular program or wouldn't necessarily be seen as being the kind of thing you bought in the first place? They might be additions to how it works technically as opposed to simply having a new functionality or something like that.

● (1635)

Mr. Mike Lake: I think Mr. Sookman wanted to jump in there as well.

Mr. Barry Sookman: Yes, I was going to make a point. It's really that since we've had a chance to review the bill, we've been able to identify some situations in which the installation of a computer program might be problematic, either because it's not practicable to get an express consent in every case, or because there are situations where it's not possible to comply with the form of the consent because in order to get it there have to be certain disclosures. There have been difficulties in terms of how one would comply with the obligation to provide information about every single update in advance when you're contracting today for updates that may occur over the course of a year.

But if I could make one last point, it is this. We really have to recognize that computer programs today are used in every digital device. This is not only about computers and the Internet. It's about computer programs that are loaded into cameras and into every device that is networkable today. There's a real issue about being able to define in advance a new regulatory regime to deal with computer programs on digital devices.

The Chair: Thank you very much, Mr. Lake and Mr. Sookman.

We'll now go to Mr. Masse.

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

Thanks to the delegations for being here today.

Getting into this has been an interesting debate, because I think one of the things that Canadians often forget is their rights. We're the ones who purchase our computers and our electronic devices. We pay monthly fees for them. We pay to maintain them. At the same time, they have become portals for marketing and advertisement, something that is an invasion, I believe, in terms of costs that you have to incur.

I'll start with Mr. Sookman and one of the things I'm concerned about.

Maybe you could expand on this. It's the issue of implied versus express consent. Once again, I've made that investment and I basically control the machinery I'm using. It would seem to diminish my capabilities to prevent unsolicited commercial and other types of advertising if we move to implied consent, because then we've put that into a third party's hands versus our own. I don't think it's too onerous to get that express consent given the fact that you can do so through a multitude of different venues, whether it be through the Internet itself or even through direct regular mail and so forth.

Perhaps you can expand upon that and my concern about vulnerability if we take that away.

Mr. Barry Sookman: There's been debate since at least prior to the year 2000 about the appropriate form for getting consent with respect to the use of people's information, which would include address information. People had that debate back in 2000 when we were debating PIPEDA and what form of consent should be used for privacy legislation.

I think everybody sitting at this table has the highest regard for the need to respect privacy and personal information. At the time that was debated, there was a consensus that the privacy legislation would still be effective if it had a mix of both express and implied consent. At the end of the day, what was accepted as part of the CSA model code was that for very sensitive personal information, as a practical matter, only express consent was sufficient, and for less sensitive information, it would be appropriate in certain cases to use implied consent, which is part of PIPEDA. That's what Canadian business operates under today: this standard that can vary from information to information.

Now, many companies will use express consent. Many companies, where they have the opportunity to deal with individuals, have consent as part of their privacy policies. I have no doubt that those companies will continue to do that whether we're dealing with PIPEDA or the ECPA. So for those I think there is not going to be a change.

The issue, though, is when we move to a regime that basically says “thou shalt not send to anyone an e-mail that has any commercial purpose”. There are going to be many situations in which people will want to receive e-mails from others. It would almost go without saying that they would want to receive e-mails from others. By imposing that express consent where there hasn't been that opportunity, what we do is take away from the usefulness of the medium.

For example, in many cases we can make telephone calls to others. I could call you, tell you I'd like to sell my boat, and ask you if you would be interested in buying it. Maybe you're not my friend or a family member, but maybe you're a friend of my friend or you're my sister's friend. In that situation, there's a great likelihood that I couldn't do that if this bill were enacted in this way.

So again, I think there are pragmatic reasons why implied consent would be useful.

● (1640)

Mr. Bernard Courtois: I would just like to add some practical examples. Since the bill was put forth, I have observed that a couple of people who I've known for many, many years have left, say, the government or another firm and started a business on their own. I've never had a contract with these people, but I am very happy to see their coordinates now and that they've started a firm, and if we ever.... I would never feel shocked. Actually, I find it useful to find this.

The other thing is, suppose I bought a product three years ago and I get a product recall notice or safety information. That's more than 18 months ago. Surely we don't want to prevent that.

So what we're talking about is not to open up a flood of unwanted commercial e-mails, but just to define it so that we don't capture in the definitions things that everybody would say, oh, yeah, we don't want to prevent that.

Mr. Brian Masse: No, and I agree on that element.

I guess I'm still a little bit worried, though. In the case where you are calling me, I could put it on the do-not-call list. I have a choice there.

And we do have some situations where the privacy legislation does cover us. But then again, not every citizen wants to go through that ordeal in protecting their personal privacy that way. Maybe lawyers can do it together a lot more comfortably than individual citizens can.

But specifically, will this weaken the individual person's ability to control what goes onto their devices, if we move to implied from express consent?

Mr. Barry Sookman: I don't think it will, because I think we'll have a mixture of express and implied consent. When you look at the notion of implied consent, we can still put some words around it, as they've done internationally, so that implied consent arises from something—from a business relationship or some other relationship—to make sure it's not completely open-ended. But again, that's very different from saying I can only send an e-mail to someone who has bought something from me in the last 18 months—which is exceptionally narrow—or I can only send an e-mail to someone who is an immediate family member, as opposed to someone else.

Mr. Brian Masse: Okay. I'd like to spend the rest of my time, Mr. Chair, asking Mr. Hill a question about something that hasn't been followed up.

I would like you to expand a little bit on the do-not-call list as part of this legislation. You've expressed concern about that being tagged on to this. Perhaps you can explain a little bit more about that.

There has been a similar expression of concern by other witnesses who have come forward, who thought it could trigger another process or piece of legislation, and that this bill right now might actually make things more complex.

So perhaps I'll give you a moment to reiterate those concerns.

Mr. Wally Hill: Thank you.

The do-not-call program has only been in operation for about eight months now. Our feeling is that it's important to give that program an opportunity to run for a reasonable period of time so that it can be properly evaluated. The original legislation provided for a report back to this committee on the operation of the do-not-call list. We'd be very concerned about including in this legislation, as almost an afterthought, a provision that would effectively allow the government, at the stroke of a pen at some later and not-defined date, to eliminate the program without the kind of discussion we feel would be warranted.

Even now, having heard of these provisions in the bill, we have members asking us, is it true? Is this program going to be pulled out or turned off? We think it creates uncertainty for the business community to have this kind of a trigger placed in the legislation. We just feel it's not necessary to the thrust of the Electronic Commerce Protection Act.

Granted the minister's argument that convergence may at some point yield an argument to make some changes, but I think at that time we would suggest that legislation be brought back and the situation be looked at then.

● (1645)

Mr. Brian Masse: Do any other panel members have any comments or a position on the do-not-call list as part of this?

Okay.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Masse.

We'll now go to Mr. Garneau.

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

I'd like to direct my questions to Mr. Sookman, given his expertise in this area. I'm going to refer to some comments made by Professor Geist, whom we had the pleasure of hearing last week, and who in fact wrote and sent me a blog about it. I'd like to hear your comments, Mr. Sookman, on his responses to specific issues and questions that were asked at the last meeting.

I'm reading from his blog here. One of them was:

> Why has Australia targeted direct marketing as its focus in its legislation while Canada talks about commercial messages?

His answer was:

> Australia has not done that. Both laws use commercial electronic messages.

What would be your comment on that?

Mr. Barry Sookman: In his testimony—and I think I did see the blog you're referring to—Professor Geist indicated there was no distinction between the ECPA and the Australian legislation, since they both used the same term.

Well, the fact is they use the same defined term in name, but the definitions are actually different. So while they use the same term, in Australia they define it as a specific series of acts that are direct marketing, whereas the Canadian bill, which would include a long list of items—very similar to Australia's—adds this general principle that it could incorporate anything broader.

So they're the same in name but not in effect.

Mr. Marc Garneau: Okay.

The next one is: does the ECPA extend its jurisdictional reach too far beyond Canada's borders? I asked this question. His answer was: "The law requires a connection to Canada to apply. This is consistent with jurisdictional law more generally that mandates a real and substantial connection."

What would be your comment on that?

Mr. Barry Sookman: I know a little bit about the real and substantial connection test because I argued the leading case in the Supreme Court of Canada that applied it in the Internet context, and that test has absolutely nothing to do with the interpretation of the territorial scope. The fact is this bill includes routing as being an element that would make foreign direct communications—that is, from a foreigner to a foreigner, an American to an American, not accessed by a Canadian, not sent by a Canadian to the U.S.—subject to the act.

So I think the issue really is the principle's international comity. Should we be extending our legislation to cover matters that really and essentially are only communications between foreigners? To do so would actually have significant detrimental effects on Canadian companies, because there are Canadian companies that actually route, as part of their service, all messages through their relays, which are in Canada, and that would mean that their foreign customers would have problems using certain Canadian companies, and the Canadian companies would have to then move their relays outside of Canada to enable foreigners to use their service.

So I disagree with that comment.

Mr. Marc Garneau: I asked another one about e-mail harvesting provisions, specifically whether law enforcement would be impeded due to the restrictions on e-mail harvesting. His answer was: "Unlikely. While the ECPA alters PIPEDA to address email harvesting, the numerous police powers to access far more than just an email address remain unchanged."

Mr. Barry Sookman: Again, I would disagree with that assertion.

First, PIPEDA set out generally applicable principles that permitted the collection, use, and disclosure of information for the purpose of enforcing Canadian law, and very specifically enabled disclosures for the purposes of complying with subpoenas, warrants, and court orders. Those are the exceptions that courts look to when making orders. Should the law be changed and should these generally applicable exceptions not apply, it could well be argued that law enforcement would not be entitled to the information, because it would be protected by the act.

I have heard concerns from the enforcement community about this, and I think they are extremely concerned that there was the potential here to impede law enforcement on the Internet. Private individuals are concerned as well.

● (1650)

The Chair: Thank you very much, Mr. Garneau, for those questions.

Mr. Sookman, thank you.

Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you very much, Mr. Chair, and thank you to our guests for coming this afternoon.

Mr. Sookman, I'd like to follow up with you, just for my own education. Are you representing the Canadian Chamber of Commerce today?

Mr. Barry Sookman: Yes, I am.

Mr. Mike Wallace: So you're a member of the chamber? They're not your client, as a lawyer?

Mr. Barry Sookman: McCarthy Tétrault is a member of the chamber.

Mr. Mike Wallace: Has the chamber put together a review committee of some sort to look at spam or these kinds of things? People are looking to you as an expert, have actually called you an expert. I want to know about your background and why that is.

Mr. Barry Sookman: Okay.

Sue.

Mrs. Susanna Cluff-Clyburne: I was going to say that Mr. Sookman sits on our e-com telecom committee as a member, and he is participating with us today because he is an expert on—

Mr. Mike Wallace: So he's representing the chamber; whatever he says is the chamber's position. Okay.

Mr. Barry Sookman: When the bill came out I also did a memo for the chamber, summarizing its effects on the members.

Mr. Mike Wallace: It was just because I saw the name of the law firm and I didn't know if you were here with them or what. I might have missed that at the beginning, I'm sorry.

I think we heard from virtually everybody that, in principle, you agree with the bill. Is that an accurate statement or not, or am I misinterpreting what people said? In principle, you agree with the bill. A nod of heads is fine with me, yes or no.

There was a discussion about further discussion. My understanding is that this discussion has been going on since at least 2005, if not before, so in my view I think it's time we moved on.

I actually am a little confused about the discussion between you, Mr. Sookman, and Mr. Courtois. I'm of the view that the broader net, as people like to call it here, is the appropriate way, and that we do make some clarifications on implied consent, and so on and so forth, to be able to capture that. I'm not sure if you agree with that approach, Mr. Sookman, or if you would like to see it much narrower and go in the other direction. Am I reading that testimony accurately or not?

Mr. Barry Sookman: I'm saying two things. The first thing is that the definition itself of what's caught could be narrowed, as it is in every other jurisdiction that deals with this, so as not to inadvertently catch a wide net. The second thing is to expand the implied consent as well.

Mr. Mike Wallace: Right. Okay.

Unfortunately, I was away last Thursday when we dealt with this bill, but in the previous meeting I was here as a member of the industry committee. I asked specifically the minister and his officials about a five-year review. I remember you had talked about whether we should do this and that this might happen. Some change might happen; it might be an issue. The word “might” comes up quite a bit. In my view—I've been here only three years, and I was on the PIPEDA review—for us to have a bill, we would be here forever trying to get it absolutely specific and nothing would happen, not just here in this committee but in government in general.

My suggestion was that we would have a five-year review so that we put this in place, we get this passed, we get it operating, and we get the regulations in place, which obviously takes some time afterwards. In the bill right now there's no such thing as a five-year review. I would like your opinion about whether an addition of a five-year review would be worth it or not to this particular piece of legislation.

I'll take anybody's answer.

● (1655)

Mr. Bernard Courtois: Yes, I think a five-year review will be useful. These are things that change significantly. I would say, however, that you have to put flexibility in the bill right now, because there can be a lot of harm caused on one side or the other during those five years that you don't want to happen. So you need to set it up correctly going in, and yes, you can review it after five years, but you have to have the flexibility in the bill itself. For example, you say we have been debating this since 2005. I was on that task force. As I say, we spent a lot of time just on the basic principles of spam, opt-in versus opt-out. We spent no time covering these kinds of provisions because we had never seen them, of course. We thought something should be done about spyware, but even the task force didn't go down to say, how exactly do we approach that?

What we want now is not to have the case of the person I've known for 20 years go and set up their own firm and all of a sudden he's susceptible to $10 million in civil lawsuits for sending out notices that I want to receive—as to where they're operating from now—or for things that can be downloaded onto my computer, or for perhaps the kind of unsubscribed mechanism that you can do on the computer that is not going to work well on the BlackBerry.

Mr. Mike Wallace: Sir, do you think that's actually definable in a piece of legislation, to get to that fine detail?

Mr. Bernard Courtois: In the sense that you can define “implied consent” in a way that at least you know you haven't covered the bad stuff. You can define the types of bad behaviour that you're going after so that you know you're not going to catch some of the good behaviour. That's why I'm saying you need a provision there that says if there's some new bad thing that comes up that we have not foreseen—and of course the bad guys are always trying to think up new variations as well—you put in the regulation that you can cover that. So it's going to happen for a month, or two or three, and you've covered it.

What you can't do is inadvertently catch something day in and day out that is perfectly legitimate and take three months to correct that.

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

We'll now go to Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): Thank you, Mr. Chair. I'd also like to welcome the witnesses.

My question is for Mr. Sookman. I think you are caught in the middle, so to speak. You represent the Chamber of Commerce, whose members include industries. You spoke of business to business contacts and all of the members of your association that want to send e-mails. However, at our last meeting, mention was made of a problem. The fact is that many businesses do not like to receive e-mails, even those sent by another business. Take, for example, someone who has a contract to build a 10-storey building. Suppose door and window manufacturers across Canada and the United States decide to e-mail this business and it receives about 500 e-mails in all. There is a cost to the business because someone needs to open and read all of these e-mails. Time is lost in the process.

How do your partners feel about this? In a way, they are not in a conflict of interest situation, but in another way, they are because they can no longer send out an e-mail without violating the terms of this act?

[*English*]

Mr. Barry Sookman: I think it's true that some businesses will not want to receive certain business e-mail. The objective here is to find the right mix, because many companies would.

Many companies—in fact, many members of the chamber—establish websites for the very purpose of developing a relationship with those they don't know yet. They have a description of their products and services. They publish their e-mail addresses and very much welcome a new supplier or a new buyer of their products and services. This is a situation where there is no pre-existing relationship. Those companies have made investments for the very purpose of having people they don't know contact them to buy these new Canadian products or services. They would be delighted to get these e-mails.

As the bill is currently drafted, because of the express consent, they wouldn't even be able to click on the e-mail address that's on the website for the purpose of communicating with them, making an order, or sending them an RFP or RFQ. I think that's the problem we're trying to solve. The implied consent rule would help in that kind of situation.

Australia deals with that situation by recognizing an express exception for e-mail addresses that are conspicuously published on websites.

● (1700)

[*Translation*]

Mr. Robert Vincent: You say that some people are happy to receive these e-mails, but what about the businesses that are unhappy over the large number of e-mails they receive? What do you say to those who do not want to receive spam?

You are on the horns of a dilemma. You claim that a balance needs to be struck, but it only works one way. The people who want to receive e-mails from business associates ultimately end up getting e-mails from people with whom they do not want to associate.

How do you strike a balance? A business will no longer be free to choose the party with whom it wishes to associate because it will be receiving between 500 and 1,000 pieces of spam per day, unless it hires someone to open these emails all day long to see if they contain any interesting offers, or chooses to open them itself to see if there is anyone they may want to work with.

How do you respond to that? How is it possible, in your opinion, to strike a balance? I consulted you website to see the recommendations put forward by the Chamber of Commerce. You haven't mentioned a single one of these recommendations today.

[*English*]

Mr. Barry Sookman: This is a circumstance that many Canadian businesses are confronted with, and what we're suggesting would actually protect those businesses. They aren't the businesses that are establishing websites and saying, “E-mail me. Here's my e-mail address.” You're referring to businesses that aren't doing anything that would invoke business relationships or implied consent situations. The regime I'm suggesting would protect those businesses you're referring to, because they receive e-mail, there's no express consent, and there'd be no way to even argue an implied consent. So I think the situation would be adequately dealt with.

The Chair: Thank you very much, Mr. Sookman, and, *merci, Monsieur Vincent.*

Mr. Lake.

Mr. Mike Lake: If I could, I want to deal with the question of the administrative monetary penalties. I think Ms. Morin brought this up. As I was looking at clause 20 here, in terms of the issues, there was some talk of someone not being able to afford a million dollars or $10 million, but when I read subclause 20(3), “The following factors must be taken into account when determining the amount of a penalty”, it seems eminently reasonable to me that the things we take into account are: “(a) the purpose of the penalty; (b) the nature and scope of the violation;” (c) and (d) “the person's history”; “(e) any financial benefit that the person obtained from the commission of the violation”—that seems to make sense; “(f) the person's ability to pay the penalty”—that makes some sense; (g) whether they “voluntarily paid compensation to a person affected by the violation;” or “any other factor”.

So it seems as though we're kind of covered there. I don't think there'd be a concern that someone, the first time they committed an offence, would wind up getting a bill for a million dollars, or a company for $10 million.

Maybe comment on that. Do those clauses there seem like a reasonable approach to this?

Mrs. Suzanne Morin: As I mentioned in my opening comments, I think Industry Canada went to great lengths to try to diminish possible negative consequences on business and those who might make a mistake, or who really aren't the ones who are filling up inboxes of individual Canadians, or citizens around the world for that matter, or Canadian businesses. But it's still placing Canadian businesses in the position of having to now comply with what is in essence a new and potentially overlapping regulatory regime, because a business, large or small, still has to defend itself before the regulator, which is the CRTC in this case, or the Competition Bureau, or defend itself before a private right of action. There are definite provisions for undertakings. I've had people e-mail me and ask me, what's an undertaking? Does a small company actually know what it means to do that?

There's no doubt that over time the regulator would come up and develop those practices, but for those types of situations, the ones that really aren't harmful—these aren't the ones that are filling people's inboxes—we have a perfectly legitimate privacy regime that works. So it's just flipping it on its head a little bit, if you like, and rather than have the legitimate company have to defend themselves, it could also be that all those factors that you listed, those are the things you use to nail the ones who are flaunting the law.

● (1705)

Mr. Mike Lake: I have a very short time, so I'm going to move on, but it seems to me that this is more working with the existing privacy legislation than against it.

Mr. Sookman, there are a couple of articles from something called SPAMfighter News, and I have to say I'm not really familiar with the publication, but I was interested to note some of the ideas that were attributed to you. This wasn't a direct quote from you, but it certainly attributed the thought to you that relatively new software developers delivering e-mail queries to those distributors with whom they never had a business relation could also be detained. That seems rather harsh. I don't see anything in the legislation that talks about people being thrown in jail for this.

Mr. Barry Sookman: I never said that.

Mr. Mike Lake: I just wanted to clarify that. It did say in the paragraph, "Sookman noted that", and went on to kind of attribute the thought to you, so I just wanted to get some clarification.

Mr. Barry Sookman: I have problems with the inaccuracy of the—

Mr. Mike Lake: Okay.

You don't really think the law would ban Canadians from using the Internet? There might be a tweak or two needed to fix a few things, but we're not talking about an Internet ban for Canadians, are we?

Mr. Barry Sookman: There's a question about whether the bill would be applied literally—do what it says, as anyone would ever interpret the actual words—or whether somebody would step back, look at the spam report, and say, "Oh, my goodness, nobody ever intended that."

Look at the spyware provision, as an example. It says you need express consent before any computer program can be installed on a computer. When I first saw those words, I thought, "Oh, my goodness", because when you think about how the Internet works, code is loaded into browsers, and the instant a web browser hits a site, if it's a Java program, you have Java programs installed in a browser. Or if the site is developed using HTML code, the second the browser hits the site, you have HTML code installed.

Taken very literally—although I have no doubt that nobody intends this, since it would be impossible to get express consent prior to actually accessing the website, unless website operators were going to try to get consent from everyone who might possibly use them in some other medium—then technically it could have that far-reaching effect. I think people realize that needs to be fixed. I don't think the fix is to rely on some web browser setting, as one suggested, because that's not a technologically neutral fix. It deals with only one situation. This is a more generic problem.

Again, I think the bill can be fixed so this doesn't happen. If that section targeted only malware, it would not be a question.

The Chair: Thank you very much, Mr. Lake and Mr. Sookman.

Mr. Masse.

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

On that subject matter, when I first saw the bill, I thought, "Geez, maybe Microsoft might actually have to release a platform that worked when they had put it on the market first."

Voices: Oh, oh!

Mr. Brian Masse: In all seriousness, do you have a specific suggestion in terms of that? Is it just to put in malware? Is that it? Is that the end-of-the-day suggestion that we would have? And wouldn't that then open us up to other problems?

Mr. Barry Sookman: I think when you look at the balance between trying to prohibit perfectly benign and beneficial programs and then trying to work your way out of it through, potentially, regulations that don't exist today to cover that situation, or trying to identify what really is a problem, it's a lot easier to define what malware is, because people know it, and then to leave the regulations available, as Mr. Courtois was saying, to be able to expand it.

I really do think there's going to be more variation and diversity in the use of different kinds of computer programs that are benign and useful on the Internet than there are going to be innovations in spammers. I think through diligent regulation we can deal with the new innovations in spammers, but I do have real concerns about dealing with legitimate innovations and making them legal one after another. I think that is very difficult.

● (1710)

Mr. Brian Masse: To all the panel, I'd like to hear if there's consensus or support for the current structure of the 18-month contact and the provisions around that. We haven't heard a lot about that.

Is there a comfort level, the way the bill is currently structured, in terms of the 18-month business contact and personal contact?

Mr. Bernard Courtois: I think I expressed the fact that I find it awkward that people I've either had a contract with...or certainly that people wouldn't buy a product more than 18 months ago. I think 18 months might have been useful in other contexts, but here, I think, what you're trying to distinguish between is e-mails that you don't want to receive and e-mails that you do want to receive.

I think 18 months is an arbitrary cut-off. I can have a relationship that's well over 18 months, and I want—

The Chair: Mr. Courtois, excuse me. We have a point of order.

Mr. Mike Lake: Mr. Chair, can I just have Mr. Masse, Mr. Courtois, or maybe even an official from the room point out where that is? I don't believe that's part of the legislation, this 18-month express consent issue that's being brought up.

The Chair: Thank you very much, Mr. Lake. That is not a point of order.

We'll continue with Mr. Sookman and Mr. Masse.

Mr. Bernard Courtois: In the definition, paragraph 10(4)(a) refers back to subclause 10(3), and it says:

> the purchase or lease of a product, goods, a service, land or an interest or right in land, within the 18-month period immediately preceding

The Chair: Okay, thank you, Mr. Courtois. That's not a point of order, but thank you for addressing the question.

Mr. Masse, go ahead.

Mr. Brian Masse: I know there were some things...for example, a real estate agent or an insurance person might move companies and so forth, and we may have to look at those situations.

I want to make sure the other people at the table get a chance to comment on this as well.

Mr. Wally Hill: We are comfortable. This is a definition of the existing business relationship. It's a definition that was worked out in discussing another marketing channel, and we feel it can apply equally in this instance.

Ms. Barbara Robins: I'd just like to say I think it definitely can apply, because we have it in here, but you may want to have a look at, for example, New Zealand's law, which refers to the term of consent that can reasonably be inferred—so whether we're talking about inferred or complied...the conduct in a business and other relationships of persons concerned. It has a more open and flexible definition, as opposed to 18 months, which in certain circumstances may or may not appear to be arbitrary. There are other laws that do provide slightly more flexible language to imply an inferred or deemed consent.

Mr. Barry Sookman: Yes. You heard my comments previously about what the regime should be.

But if we were focusing on the term "existing business relationship", one thing that would be useful to keep in mind is the background, where this definition came from. It came from the Telecommunications Act, and it preceded the establishment of the do-not-call list. This definition has more usefulness in the business-to-consumer market, which is what it was more designed for. The prospect now is taking the same definition, without recognizing that the same definition is also going to be used in a business-to-business context. The business-to-business relationships are much more diversified.

If the intent is to go with the definition, my suggestion would be to examine this particular definition and see how it needs to be adapted to really deal with business-to-business as opposed to only business-to-consumer.

● (1715)

Mr. Brian Masse: Mr. Hill.

Mr. Wally Hill: I think we disagree on this point. There is a business-to-business exemption or exception in this bill, so the implied consent component is designed for business-to-consumer interactions. Business-to-business marketing, where it concerns the interests of a business that's receiving the marketing, is excepted by this legislation.

Now, in my opening remarks I pointed to that and indicated that in discussions I've had there's been some concern that the definition in the bill as it now sits may be a bit too narrow. I think we should look at some alternatives, and I've mentioned the Alberta legislation.

I don't think that's the concern that's being suggested on that point.

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

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

We're going to go briefly to Mr. Lake, and then we're going to suspend to allow our witnesses to leave us, and we're going to briefly discuss future committee business.

Mr. Lake.

Mr. Mike Lake: In reading this, and having heard conversations as we've been talking through this, I think it's important to talk about the difference between implied and express consent. There seems to have been a misinterpretation by some, not necessarily today but throughout this committee, that the 18 months refers to express consent. The reality is that if somebody buys a vehicle, or a house, or something like that, and has express consent, that express consent is good for an indeterminate amount of time, until someone actually says they don't want anything anymore. That 18 months does not apply in that situation, and it seems there may be some confusion around this. This situation we're talking about, the 18 months referred to here, refers only to implied consent. I just wanted to make that clarification as we're thinking about this as we move forward.

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

I want to thank our witnesses from the four different organizations for appearing in front of us today. We appreciate your testimony. It will be helpful as we continue our review of this bill.

We'll suspend the meeting for five minutes to allow people to leave the room so we can talk about future committee business in camera.

The meeting is suspended.

[*Proceedings continue in camera*]

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
