House of Commons
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 030 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, June 18, 2009

Chair

The Honourable Michael Chong

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

http://www.parl.gc.ca

Standing Committee on Industry, Science and Technology

Thursday, June 18, 2009

● (1535)

[*English*]

The Chair (Hon. Michael Chong (Wellington—Halton Hills, CPC)): Welcome to the Standing Committee on Industry, Science and Technology and to our 30th meeting this Thursday, June 18, 2009. We're here pursuant to the order of reference of Friday, May 8, 2009, to study Bill C-27. Before us today we have two organizations: the Office of the Privacy Commissioner of Canada and the Competition Bureau.

From the Office of the Privacy Commissioner of Canada, we have Madam Denham, who is the assistant privacy commissioner of Canada.

From the Competition Bureau, we have Mr. Duane Schippers, who is the deputy commissioner of competition of the legislative and parliamentary affairs branch.

I'd also like to mention that we have Mr. Baggaley from the Office of the Privacy Commissioner. He is their strategic policy advisor.

Welcome to all of you.

We'll begin with opening statements, beginning with the Office of the Privacy Commissioner of Canada.

[*Translation*]

Mrs. Elizabeth Denham (Assistant Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair and members of the committee, for inviting our office to address you on this important government initiative. I am Elizabeth Denham, Assistant Privacy Commissioner, and I am joined today by Hedy Kirkby, Acting Senior Legal Counsel and Carman Baggaley, Strategic Policy Advisor.

[*English*]

The Office of the Privacy Commissioner of Canada has long called for anti-spam legislation. We welcome and support the introduction of the Electronic Commerce Protection Act. This is an important piece of legislation that addresses a serious problem. Much more than a mere nuisance, unwanted electronic messages—or spam—have significant consequences for our economy. Spam affects productivity and undermines confidence in electronic commerce.

This legislation has the potential to help individuals and organizations deal with unsolicited electronic messages, and it also provides important redress mechanisms, including a private right of action. We believe it strikes the right balance between giving people greater control over the e-mail and text messages they receive, while still allowing legitimate businesses to continue to communicate with their clients and their customers.

In the run-up to the development of PIPEDA more than 10 years ago, concerns were expressed by businesses that are similar to those we've heard in this debate about ECPA. However, interestingly, in the PIPEDA review just two years ago, the business community did not raise the same concern that privacy rules would impede business. Business is adaptable. There's evidence that there's a competitive advantage to giving consumers choice and respecting their privacy. As well, for businesses that have actually been complying with PIPEDA for the past nine years and respecting the privacy of their customers, this law should have little or no adverse effect.

The legislation will help us fulfill our mandate to promote the protection of personal information. E-mail addresses are considered personal information under the Personal Information Protection and Electronics Documents Act, PIPEDA.

Our office is concerned about e-mail addresses being collected and used to send spam without consent. We're also concerned about the growing use of spam e-mails containing malware or spyware to collect personal information in order to commit fraud such as identity theft. I should also add that we see this legislation as complementing Bill S-4, which would amend the Criminal Code to deal with identity theft and related misconduct.

The CRTC, the Competition Bureau, and our office will share enforcement of the act. We look forward to working collaboratively with these two agencies and Industry Canada in carrying out our new responsibilities, including that of educating the public about this important new legislation. ECPA contains provisions to facilitate consultation, referral, and information sharing among the three agencies to enable more effective and efficient investigations and enforcement actions.

The three agencies will also have the authority to share information under written arrangements with foreign states where the information may be relevant to an investigation under a foreign law that addresses substantially similar conduct. This is an important provision that's going to help us deal with the challenge of a problem that really knows no borders.

The CRTC and the Competition Bureau will have shared responsibility for enforcing the anti-spam provisions, and those are the provisions dealing with the sending and the content of electronic messages. The Privacy Commissioner will have responsibility for investigating related contraventions of PIPEDA, specifically, the unauthorized collection and use of personal information through e-mail address harvesting, dictionary attacks, and the use of spyware to collect personal information.

● (1540)

The legislation will not change the existing enforcement powers of the Office of the Privacy Commissioner, nor is it expected to create a significant increase in complaints to our office. We actually anticipate that many complaints are going to be directed elsewhere, to the CRTC and the Competition Bureau.

The bill also imports two significant sets of amendments that have been discussed in the context of the review of PIPEDA. Under the first set of amendments, the Privacy Commissioner will have the discretion to decline to investigate a complaint—something we don't have now—or to discontinue a complaint investigation, including in cases where the matter could be more appropriately dealt with by the CRTC or the Competition Bureau.

Under the second group of amendments in ECPA, the commissioner will have the authority to collaborate and exchange information with provincial counterparts—not just those with substantially similar legislation—and with foreign counterparts who enforce data protection laws that are similar to PIPEDA. To be clear, these amendments apply to all our activities, not just those related to spam.

Under the proposed amendments to PIPEDA, the commissioner may decide not to accept a complaint if she believes that the complaint could be more appropriately dealt with under other available procedures. This includes procedures provided for under federal or provincial laws or grievance or other procedures. A complaint may also be refused if it is not filed within a reasonable amount of time—the evidence has gone stale—from the date when the issue actually arose.

The commissioner will notify complainants and also the responding organization if she decides not to investigate a complaint, and she'll provide reasons for her decision. The commissioner may reconsider a decision not to investigate if she is satisfied that there are compelling reasons to do so.

As well, ECPA provides the commissioner with the discretion to discontinue some investigations if she is of the opinion that there is insufficient evidence to pursue the investigation or if the complaint is trivial, frivolous, or vexatious.

The Office of the Privacy Commissioner of Canada has previously asked Parliament in the context of the PIPEDA review to provide the commissioner with the discretion to refuse or to discontinue complaints.

This is important because traditionally privacy issues have arisen in the context of interaction between one person and an organization. They have come to light as a result of a complaint by an individual. More and more often, however, critical privacy issues are arising from systemic threats, from rapidly advancing information technologies, including Internet applications and surveillance. This discretion to refuse and/or to discontinue complaints will, importantly, allow our office to focus our investigative resources on privacy issues that have broader systemic interest.

In closing, I would like to thank the committee for providing us with the opportunity to explain our role in enforcing this important new legislation and the reason we believe this initiative is going to help the office better protect the privacy interests of Canadians.

I would be happy to take your questions.

[*Translation*]

I would now be pleased to answer your questions.

The Chair: Thank you, Ms. Denham.

[*English*]

We'll now hear from Mr. Schippers from the Competition Bureau.

[*Translation*]

Mr. Duane Schippers (Deputy Commissioner of Competition, Legislative and Parliamentary Affairs Branch, Competition Bureau): Good afternoon everyone.

Thank you, Mr. Chair, for inviting the Competition Bureau to appear before the committee to discuss Bill C-27, a legislative initiative that targets spam.

[*English*]

It is rare that one finds an idea or a point of view that almost every Canadian can agree upon. Unsolicited electronic communication, or spam, is one of the most universally reviled features of the Internet age. While its most malicious forms may be designed to spread viruses or facilitate identity theft, a significant proportion of spam involves the false or misleading promotion of products or services, particularly in the health and financial sectors.

[*Translation*]

For those less familiar with the Bureau, our mandate is to protect and promote competitive markets and to enable informed consumer choice in Canada. Our principle statute, the Competition Act, allows us to carry out both civil and criminal enforcement against, among other things, deceptive marketing practices.

● (1545)

[*English*]

With the passage of Bill C-10, the law implementing the federal budget, the penalties for deceptive marketing practices under the Competition Act were strengthened, both in terms of the monetary penalties and through the introduction of restitution orders to get victims their money back. These amendments were designed to harmonize the act with our international counterparts and to improve the bureau's ability to promote truth in advertising.

[*Translation*]

The proposed legislation before you, Bill C-27, the Electronic Commerce Protection Act, would amend the Competition Act to allow the Bureau to more effectively combat false or misleading advertising in electronic communications and better protect the integrity of electronic commerce in Canada.

[*English*]

Along with the CRTC and the Office of the Privacy Commissioner, the bureau would be one of three partners carrying out responsibilities under this initiative.

[*Translation*]

The 2005 report of the Task Force on Spam established by the Minister of Industry identified "gaps in current Canadian law that must be filled". As it stands now, the Competition Act contains both civil and criminal provisions to curb the use of false or misleading advertising.

[*English*]

However, Canada still has no equivalent to laws found in other industrialized countries that relate specifically to electronic commerce, such as the CAN-SPAM Act in the United States or the Spam Act in Australia.

[*Translation*]

The additions to the Competition Act outlined in Bill C-27 would help to clarify more precisely what cannot be done in electronic messaging and how competition laws would apply in cyberspace.

[*English*]

Specifically Bill C-27 would add more targeted civil and criminal provisions with respect to false and misleading advertising in electronic messages. It would provide authority for court injunctions to restrain conduct that falls within these new provisions and make certain that the act is technologically neutral. False or misleading representations in header information, such as subject lines or sender names in e-mails, in the content of the communication itself, or in locators, such as web addresses or URLs, would now be more broadly covered.

[*Translation*]

An example of a message that we have all received is one in which the subject line suggests that the message is a greeting from a familiar friend or trusted business, but whose content turns out to be an advertisement for a dubious product from a less than reputable source. This activity would fall under the new provisions as a false or misleading header.

[*English*]

An e-mail or text message advertising a bogus fuel additive, for example, falsely claiming to double your car's fuel efficiency, would be an example of a false or misleading representation made in the content of a message.

[*Translation*]

Similarly, a Canadian website that chooses a domain name or search terms to suggest that it is a source of job opportunities when it is merely a collection of links and vague advice would be caught under the "false or misleading locator" provisions.

[*English*]

While these examples may be covered to some extent under the current act, Bill C-27 would make it clear that they are, thus making it simpler and faster to take enforcement action against these forms of misleading advertising.

In addition to administrative monetary penalties and potentially even criminal prosecution, Bill C-27 proposes to expand court injunctive powers. The bureau will be able to seek court injunctions against spammers based in Canada or using Canadian equipment to engage in false or misleading advertising, and also against those persons and businesses supplying the spammers with the equipment and services used to carry out false or misleading advertising.

To ensure that the Competition Act remains in step with technological innovation, Bill C-27 amends definitions in the Competition Act to ensure that the act applies broadly to new technologies. For example, voice-over-Internet protocol, or VoIP, and text messaging would now clearly be within the scope of the Competition Act.

[*Translation*]

Furthermore, the framework provided for in the new Competition Act civil provisions serves as the basis to empower those affected by false or misleading spam to launch private actions under the remedial scheme in the Electronic Commerce Protection Act.

This means that enforcement will be coming from all angles, not just the Bureau or its government partners. In addition to a statutory per-message amount of damages, this scheme also allows plaintiffs to sue specifically for losses incurred as a result of the deceptive communications, ensuring that victims of scams, false advertising claims and other forms of deception have a potential way to get their money back.

● (1550)

[*English*]

In these difficult economic times, we can expect to see an increase in messages targeting not only consumers but also small and medium-sized businesses, which may suffer serious financial harm if they fall prey to misleading or false advertising messages contained in spam. It is the job of the Competition Bureau to protect Canadians from this kind of activity in all economic environments and to foster confidence in an honest marketplace.

The Competition Bureau has decades of experience in conducting investigations into false and misleading advertising and working with our domestic and international partners to achieve common enforcement objectives. For example, the bureau recently launched Project False Hope, an education and enforcement initiative that targeted false or unproven cancer cure claims found online. The project has resulted in 98% of those websites targeted by the bureau changing or removing the claims at issue in order to comply with the Competition Act. As part of the initiative, the bureau worked in collaboration with the Canadian Cancer Society to produce an awareness campaign and an informative pamphlet that has reached tens of thousands of individuals.

In other collaborative efforts, the bureau has worked with domestic and international partners, such as Health Canada, the U. S. Federal Trade Commission, and the U.S. Food and Drug Administration, to combat false or misleading claims surrounding weight loss and diabetes treatments. The bureau successfully took action against almost 100 Canadian-operated websites, with the vast majority changing or removing the claims at issue in order to comply with the Competition Act.

[*Translation*]

Cooperation is key to ensuring deceptive marketers cannot hide from authorities, in any jurisdiction. Experience conducting investigations, in both the on and offline world, combined with established cooperation networks, provides the right foundation to take action against spam.

[*English*]

Technological progress is a positive and powerful economic driver, but it comes with new ways to engage in deception, and Canadian law must keep pace. The new provisions, combined with the current provisions in the Competition Act, will provide a more complete framework to facilitate more effective and timely enforcement against deceptive conduct in the electronic marketplace in all of its forms.

Canada has been without anti-spam legislation and is lagging behind our major international trading partners. These changes allow the bureau, together with its partners, to more confidently and effectively enforce the law in an undeniably problematic but complex area.

We at the bureau are enthusiastic about the prospect of Bill C-27 becoming law. I welcome the opportunity to discuss the bureau's role and respond to any questions the committee members may have.

Thank you.

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

We'll now have approximately an hour of questions and comments from members of this committee, beginning with Madam Coady.

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

Thank you very much to both organizations for taking the time to appear and giving us your considered opinions on this bill, which is certainly an important one. I think both of you have indicated that there is a fair amount of support for anti-spam legislation, to say the least, and we're going to make sure that we make the best bill possible, so I appreciate your information here today.

I'd like to start with you, Ms. Denham, and ask a couple of questions on the PIPEDA legislation and its impact, and get your opinions on some concerns that have been raised at this committee and with me privately.

One is that the scope for anti-spam in these provisions may be too broad, with the consent provisions being too narrow. If I understand it correctly, the CSA model code has been adopted by PIPEDA. Basically, it defines “implied consent” as “where consent may reasonably be inferred from the action or inaction of the individual”.

This particular legislation is different from that. It's not as defined. Do you have concerns about how the act actually deals with the provisions for consent?

● (1555)

Mrs. Elizabeth Denham: I don't have concerns about the level of consent that's required under ECPA.

Just to give you a bit of background, PIPEDA is a law of broad applications. It was created to work in a variety of situations. My view, our view, is that PIPEDA is a floor, not a ceiling, and that the form of consent in PIPEDA should be applied by looking at the sensitivity of the personal information. Express consent or opt-in consent is a higher form of consent; it's more privacy-sensitive than implied consent. I think that's appropriate here, because it's going to be effective in dealing with the problem that is spam.

Ms. Siobhan Coady: That's great. Thank you very much for the answer to that.

I want to ask a question now about your opinion of the anti-address harvesting, much along the same lines. Clause 78 of ECPA basically amends PIPEDA to create a private right of action with respect to it, and there are a number of things, including the collection and use of personal information under proposed paragraphs 7.1(3)(a) and 7.1(3)(b) of the Personal Information Protection and Electronic Documents Act.

Now, that departs from the structure—and we just talked about that—of PIPEDA in that PIPEDA recognizes that there are legitimate needs to collect, use, and disclose personal information without knowledge or consent. There has been discussion and concern raised to me that the anti-address harvesting prohibition may be too broad under ECPA in that PIPEDA doesn't trump law enforcement, but this particular act may. The scope is broader than that of some international legislation. No other international legislation prohibits the collection of address information for legitimate purposes. There is also the question, for example, of whether EPCA prohibits legitimate law enforcement.

I now ask you to put on your lens of PIPEDA, which does one thing, and EPCA, which does another, and give me your comments, please.

Mrs. Elizabeth Denham: Thank you for that question.

We haven't been consulted by law enforcement, in particular, on this issue, but ECPA as a whole does not apply to the collection of personal information by law enforcement agencies, so that's our view. It applies only to harvesting and spyware activities.

The amendment you referred to in clause 78 of Bill C-27, under proposed section 7.1 of PIPEDA, does not refer to disclosures. So it doesn't refer to a disclosure, say, from a TSP to a law enforcement organization. It just uses the term “collection and use”. That's my understanding.

Perhaps my colleague, Carman Baggaley, can add to that.

Mr. Carman Baggaley (Strategic Policy Advisor, Office of the Privacy Commissioner of Canada): I'll add just a couple of very quick points just to reiterate that since the act applies only to commercial activities, law enforcement agencies aren't engaged in commercial activity, and therefore it doesn't affect the ability of law enforcement agencies to collect this information if necessary.

The other thing it doesn't do—and I'll use a concrete example—is in regard to the cases that you may read about in the newspaper where a law enforcement agency goes to a telecommunications service provider and needs an IP address or a name associated with an IP address. There are provisions in PIPEDA that allow that to be disclosed, either under warrant or on request under paragraph 7(3)(c.1). It wouldn't have any impact on that.

Ms. Siobhan Coady: Can I use a couple of examples? Because you're using some yourself there. Do you feel that collecting information related to online harassment and stalking is fine under the ECPA? If you were involved, for example, in offline crimes like drug trafficking that might be discussed over the Internet or—I don't know even how to explain it—in some activities on the Internet related to that particular thing, do you think under the ECPA the provisions are broad enough to allow that to occur?

Mr. Carman Baggaley: A typical Internet service provider collects a great deal of information in the course of providing services. There's nothing in ECPA that prevents a telecommunications service provider or an ISP from disclosing that information that is already collected. What it does prohibit is someone specifically using a computer program to collect e-mail addresses. If they already have e-mail addresses in the course of their business, there is nothing that prohibits the disclosure of them.

Ms. Siobhan Coady: Thank you.

● (1600)

The Chair: Thank you, Madam Coady.

Monsieur Bouchard.

[*Translation*]

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

Thank you for being here this afternoon to share with us on behalf of each one of your organizations, your respective expertise.

My first question can be addressed to either the Office of the Privacy Commissioner of Canada, or the Competition Bureau. Both your organizations must work with one another, but when it comes to implementing Bill C-27, the CRTC joins forces with you.

Will your respective mandates be changed? If so, what would the changes be?

[*English*]

Mrs. Elizabeth Denham: Thank you for the question.

Our mandate and responsibilities under PIPEDA don't change under this act. Our powers don't change under the act. So I don't see significant changes in the operations of the Office of the Privacy Commissioner.

We do have the ability, under ECPA, to intervene in a private right of action. That's new to our organization. But our mandate and our responsibilities don't change.

[*Translation*]

Mr. Duane Schippers: The mandate of the Competition Bureau will not be changed by Bill C-27. It is, however, important to remember that we will work with the Office of the Privacy Commissioner of Canada and the CRTC a lot more.

[*English*]

We'll also be establishing, at some point, a spam reporting centre that should be a one-stop shopping place for Canadians to file complaints. We'll work cooperatively to handle those complaints so that Canadians don't have to try to figure out which of three organizations they should be trying to contact.

[*Translation*]

Mr. Robert Bouchard: You talk about cooperation with the Office of the Privacy Commissioner of Canada, as well with your provincial and international counterparts. The representative from the Competition Bureau also talked about cooperation.

My question is for each and everyone of you.

You talk about cooperation with institutions over which you have no authority, be they abroad or in the provinces. Will this cooperation fall under any written memorandum of agreement? Will there be a verbal agreement or an actual written and signed agreement?

[*English*]

Mrs. Elizabeth Denham: Our collaboration with provincial counterparts and international counterparts requires information-sharing agreements. Those will be established. It's based on information-sharing between other data protection commissioners who operate internationally and also in the provinces.

Right now the Privacy Commissioner has the ability to share information only with Alberta, B.C., and Quebec, because they have substantially similar commercial privacy legislation.

This broadens our ability to share information with other data protection commissioners. It also allows us to share information with an authority like the FTC and other foreign authorities that are combatting spam and have a similar requirement.

So there will be information-sharing agreements.

● (1605)

Mr. Duane Schippers: Information that's collected specifically under the new legislation is subject to these written agreements in order to share it with international counterparts.

That said, the Competition Bureau has a lengthy series of written cooperation agreements at a state-to-state level—with the United States, Japan, and other countries—as well as agency-to-agency cooperation arrangements, such as with the United States Postal Inspection Service. Across Canada at local levels we have a series of enforcement partnerships. We work with local police agencies as well as international counterparts.

In our Toronto strategic partnership, for example, we actually have the U.K.'s Office of Fair Trading as a member just because of the nature of misleading advertising representatives and how they.... They are borderless in the way they are transmitted to Canadians.

[*Translation*]

The Chair: We will now turn to Mr. Vincent.

Mr. Robert Vincent (Shefford, BQ): Thank you, Mr. Chair.

Ms. Denham, was an impact study done on the increased number of investigations you will have to carry out, given these requests? Are you going to receive additional resources to carry out these new investigations?

[*English*]

Mrs. Elizabeth Denham: We don't anticipate carrying out a great deal of investigations under this legislation. We feel that the CRTC and the Competition Bureau will probably get the lion's share of investigative work. So we don't suspect that there will be a great deal.

In terms of the funding necessary, we think it will be incremental, that, for the first year, for example, we'll need some additional funding for inquiries and communication work. We hope to be very involved, in the centre that we talked about, with public education materials and compliance education materials. Our office does a great deal of that work. We suspect there will be some increase—a handful of FTEs—for this communications work, inquiries work. The second year, we may need some new investigators.

[*Translation*]

The Chair: Thank you, Ms. Denham.

[*English*]

Mr. Schippers, just briefly reply to the question.

Mr. Duane Schippers: Thank you.

We have asked for additional resources. On the one hand, we'll be building on a base of expertise that we already have, but we will require some additional resources, particularly resources to acquire computer software and other technologies to assist us in tracking false and misleading advertising spam. We've asked for the resources, and we've been assured that the resources we've asked for will be available. But they are relatively modest increases, given the mandate that we already have to work in this area on false and misleading advertising. Our part of this tranche is really limited to false and misleading advertising.

The Chair: Thank you, Mr. Schippers.

Mr. Lake.

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

I want to start by addressing some questions that previous witnesses have had over our last couple of meetings.

First, dealing with PIPEDA, Ms. Denham, it was suggested by one of the witnesses in the last meeting that PIPEDA was sufficient to address spamming activities.

I just want to find out whether you concur with this view.

Mrs. Elizabeth Denham: I don't concur with that view.

In the experience of our office, we have investigated, I think, seven or eight complaints about harvesting e-mail addresses. The difficulty in investigating those complaints is that there is ambiguity in PIPEDA as to when express consent or when implied consent can be relied on. These are long and involved investigations. I think the clarity in the ECPA is useful, and it's effective.

Mr. Mike Lake: Okay.

Regarding the administrative monetary penalties, I will ask both of you a question. I'll start with Mr. Schippers.

In your case, I understand that the AMPs haven't changed. They're actually the same. They just use the AMPs that are already in place for the Competition Bureau. It was suggested at a previous meeting that perhaps those AMPs were too high.

Maybe you can speak to that question.

● (1610)

Mr. Duane Schippers: The AMPs that we have now are the AMPs that came about as a result of Bill C-10, the Budget Implementation Act. There was a series of changes in the act to bring administrative monetary penalties up to a level that would encourage compliance, as opposed to being a pure licence fee to engage in misleading advertising activity.

So that's what happened. For a first offence for an individual, it's $750,000 as a maximum. For a second offence, it's $1 million. For a corporation's first offence, it's $10 million. The second offence is $15 million.

Now, it doesn't mean that someone is going to end up with that administrative monetary penalty every time. The act sets out a series of factors that the Competition Tribunal or a court has to take into consideration before awarding an AMP. That includes the history of the behaviour, the isolated nature of that behaviour, the history of compliance with the act, and that type of thing.

We're also looking at the financial resources. The idea is not to create capital punishment for business when they fall offside of the legislation. The idea is to deal with false and misleading advertising in a firm manner so that Canadians can have confidence in the marketplace, particularly the online marketplace. That's an area where there is some lack of confidence. When people use their credit cards to purchase online, they want to know that what they're buying is what's been represented to them as the product being sold.

Mr. Mike Lake: Ms. Denham, on that issue, the way some witnesses have presented it is that there is a fear that a small business might have an employee who inadvertently sends out an unsolicited e-mail and the small business would get a $10 million fine or the employee would get a $1 million fine. They want to be reassured that this is not going to happen. Can you reassure them?

Mrs. Elizabeth Denham: I can, because we're an ombudsman. The AMPs doesn't apply. There are no penalties under PIPEDA.

Mr. Mike Lake: Okay, in your case, of course.

I want to talk about express consent and implied consent. One of the concerns that I've heard comes from realtors. After they sell a home to somebody, typically in the realty business cycle the person who bought the home won't be in the market to buy another home in less than 18 months. It might be four or five years. Realtors want to know that they'll be free to use their client's e-mail address to touch base with their client four or five years later, to see how happy the client is with the purchase and maintain that connection with their client. Can you reassure them that it will be okay for them to do that?

Mrs. Elizabeth Denham: My former realtor always brings me a big basket of goodies at Christmastime; I would say to add a notification and a consent to that basket. It's true that the implied consent provision in the ECPA would expire after 18 months. It wouldn't carry on for years and years.

I would recommend to the realtors that they build in that consent provision up front. I'd also like to suggest that if organizations had been complying with PIPEDA all along, there wouldn't be a problem today. These rules have been in place for a very long time.

Mr. Mike Lake: It's a simple matter of asking them for an e-mail address, and when they ask for the e-mail address, they would also ask if it's okay to contact them in the future.

Mrs. Elizabeth Denham: That's correct. Then the individual would have the option of opting out of that somewhere along the line. I think that's the proper way to conduct business in a respectful way.

Mr. Mike Lake: I'll now talk about something that has caught my attention.

Mr. Schippers, you were talking about false headers. One of the things I thought about, and I might be wrong...would that apply in the case of politicians? How about using an MP's name so that a website looks like an MP's website, but it is something completely different? I'm asking this out of curiosity.

Mr. Duane Schippers: I don't believe that an MP has ever misled anyone in his or her publications.

Voices: Oh, oh!

Mr. Duane Schippers: That said, what we're concerned about at the Competition Bureau is false and misleading advertisement to promote the sale of service or a product.

That or charitable giving activities are not the kinds of things we're focused on when it comes to misleading advertising. Our issue is commercial activities where someone is trying to create an uneven playing field in the market by misleading consumers to purchase his or her product over that of someone else who is playing fairly.

● (1615)

Mr. Mike Lake: Having worked for the Edmonton Oilers before I was elected, I was concerned about someone creating a false Mike Lake website and posting pictures of me in a Flames jersey—or perhaps a Liberal jersey; that would be a bad thing too.

In terms of the importance of this legislation, we're in a minority government context here. Thankfully we avoided an election right now, but come the fall, who knows what might happen. A few times we've seen important legislation fall by the wayside when an election is forced.

How important is it for us as parliamentarians to make sure that we get this legislation passed in terms of the global context as it relates to spam?

Mr. Duane Schippers: In terms of spam, Canada is the only G-7 or G-8 country—depending on what number one uses—without effective spam legislation. More important, given the current economic situation, what we at the bureau notice is that there is an uptick in misleading advertising activities.

For people who are unemployed, there's an opportunity for job websites to take advantage of people in these circumstances. We notice an uptick in misleading advertising. From that perspective, it's important to make sure that we have the tools so that we can deal effectively with this kind of misleading advertising.

The Chair: Thank you, Mr. Schippers.

Mr. Masse.

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

Thank you to the panel for being here.

I'll start with Mr. Schippers.

On your comments with regard to resources, I want to have a comfort zone, I guess. Will your department be looking at vulnerable groups that get targeted, such as, for example, seniors and others who sometimes are zeroed in on with some of this misleading advertising? Will you have the ability to do that?

You're indicating that you have some modest resource requests, but has there been a full evaluation, or is it just a general sense right now as to what you might need to get going to start with and then you'll do an evaluation later? Has that already been concluded? Will you get sufficient resources?

Mr. Duane Schippers: The possibility of this legislation has been a possibility for some time, so we have gone through a fairly detailed analysis of the resources we need.

On your question about vulnerable Canadians, that's already a large part of our program on false and misleading advertising. When I talk about modest resources, they really are modest. It's about giving us the extra tools to get these kinds of things, these header advertisements, so you don't have to.... You know, you're promised the free health club membership in the subject line of the e-mail, and it's only after clicking through, which is the whole objective of the spam—to get you to click through it and start reading it—that you find out there is a $1,000 initiation fee. We want to be able to take action on the first part, which is that you've misled people just by getting them to look at your product by saying it's free.

That's the kind of thing this legislation will do from the Competition Bureau's perspective. We'll still continue with our program to protect vulnerable people. In fact, the legislation is very clear, and when setting AMPs, administrative monetary penalties, and when we do criminal prosecutions, we also look very much at who is the target audience and who is the victim of the activity.

Mr. Brian Masse: That's very good.

Ms. Denham, with regard to public awareness, one of the criticisms out there with regard to the do-not-call list is that perhaps the message on how to get onto the list and how the list is used and so forth wasn't as thorough as it probably should have been for the general public, and that led to some initial problems. What type of public awareness campaign do you guys have planned for this type of initiative?

Mrs. Elizabeth Denham: I think we would obviously work in partnership with the CRTC, Industry Canada, and the Competition Bureau, but in our experience, we have found that public education and compliance education for businesses are critical to making this work.

We would definitely have our fact sheets. We actually have a blog on our site. We are now even using Twitter to get the message out to individuals who aren't necessarily the same age as most of us in the room. We would use all kinds of channels of communication. I think that's where we would invest time and resources in the first year.

● (1620)

Mr. Brian Masse: Well, we'll look forward to your YouTube video on this.

Here is an example from your presentation that I do want to use. I'm hoping you can clarify this. Under "Investigation of Complaints" in your document, which I've read through, you note that you can dismiss complaints related to other federal or provincial laws or grievances and so forth. One example you give is that it must be "within a reasonable period of time from the date...". Can you tell us what is a reasonable period of time for that and be a little more specific about why you might dismiss a complaint?

Also, then, does a complaint just basically fall off or is it referred to the other state agencies or the provinces? Is it then up to the individual to go to those other agencies that are being suggested for where the complaint should go, as opposed to yours? Or is the complaint directed by you to those other agencies or governments?

Mrs. Elizabeth Denham: As I said, the amendments to PIPEDA in the ECPA affect all of our collection, use, and disclosure of personal information across the board, not just spam. We often get complaints where someone is complaining about an incident that happened three years ago. It's very difficult to find witnesses, it's very difficult to get evidence, and it's difficult for us to spend our resources investigating that kind of complaint.

As for our ability to refer a complaint rather than take it at the Office of the Privacy Commissioner of Canada, we get a lot of complaints that we think are more properly dealt with by a labour arbitrator, or they need to be dealt with in the workplace through those processes, or by an ombudsman who works for an industry association, for example. We want other complaint resolution processes to take some of the burden off the Office of the Privacy Commissioner.

Mr. Brian Masse: Say, for example, I bring in my complaint to you, and you suggest that it needs to go to the ombudsman's office. Would you follow up with that or would you say to the person, "No, you need to call the ombudsman's office"? I guess I'm wondering whether there's tracking, whether or not they go to that place and they find a resolution or they're maybe sent somewhere else. Is any of that tracked?

Mrs. Elizabeth Denham: We've never had the capacity to refer complaints in this way. We're looking forward to the passage of this bill so we can do that. But, yes, indeed we will track the referrals of our complaints and probably give a heads-up to that organization that a complaint is coming their way.

Mr. Brian Masse: I think that's important. I know that in certain cases, especially when you're just the general public, you can get a little bit frustrated when you think you're going to the proper place to register your complaint and then you're kind of punted around. It's not that anyone means to do so; it's just that they're following the process. But if you're a general person out there, it can become very frustrating.

Mrs. Elizabeth Denham: I understand, and I think it will be very important for us to have this coordinating agency so that it is one-stop shopping and so the public doesn't get confused and referred around and around.

Mr. Brian Masse: That will be very effective for the marketing of the new program as well.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Masse.

Thank you, Madame Denham.

Mr. Rota.

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

Thank you for coming today. I would like to continue in that vein a bit, about the investigation of complaints and the complaints that come through.

Ms. Denham, I understand the commissioner has the right to determine what is frivolous and what is serious. How would that work? I'm just trying to picture it. I would come to your agency or I would come to you and say "Okay, I have a problem." I guess what I'm looking for are the guidelines or the criteria that would be used and the length of time it would it take for me to find out that my complaint or my charge would not work or would not be dealt with.

Mrs. Elizabeth Denham: Hedy Kirkby is going to answer this difficult legal question.

Ms. Hedy Kirkby (Acting Senior Counsel, Office of the Privacy Commissioner of Canada): I'd be delighted to.

Mr. Anthony Rota: I was asking was about someone who brings a charge or a complaint forward.

● (1625)

Ms. Hedy Kirkby: You mean to our office?

Mr. Anthony Rota: I mean to your office. What is the process for determining that something is frivolous or that it is a nuisance, and how long does it take for someone to realize or get an answer back that their complaint will not work or will not be dealt with?

Ms. Hedy Kirkby: We have some experience, but not very much experience, with the concept currently under PIPEDA. Under the act as written right now, while we don't have the ability to refuse to investigate or to discontinue an investigation, the commissioner has the limited ability to not finish an investigation or issue a report in a number of situations, including those in which a complaint is trivial, frivolous, or vexatious. The office has looked at it on a number of occasions as potential candidates for that situation, and my understanding is that never once have we found actually a situation that would be considered within that category. There is a reasonably high threshold legally to be able to justify rejecting or discontinuing a complaint.

Mr. Anthony Rota: I ask that because it sounds to me almost as though someone who has something frivolous or something that's considered frivolous—and that worries me even more—suddenly goes into limbo and just stays there and doesn't get dealt with. Is that how that works?

Ms. Hedy Kirkby: No, that's not how it works at all. It's looked at. It's assessed. It's measured against standards that have been set by the courts in terms of what that expression means; a decision is taken, and one continues. The process in our office has gone quite efficiently on that. Decisions were made quickly to assess that they were valid matters, that they should be investigated to the very end, and that reports should be issued. They weren't in limbo at all.

Mr. Anthony Rota: Okay, very good.

My next question is for Mr. Schippers.

On a similar note, the bureau can seek court injunctions. The complaints are filed centrally, and then you deal with any complaint yourself. The Competition Bureau takes care of that.

I'm looking at your resources. You talked about resources earlier. How much more in terms of resources will you need? And are you capable of taking care of any complaints that come forward, or, again, will they take a while?

Right now I'm thinking of a situation we have with Interac in which we're hearing that it's taking a lot longer than usual or it's taking a long period. There are some delays. You have limited resources, and I understand that. If someone complains, and there's something to be done, how long will it take or what kind of time period are we looking at? Or is that very difficult to assess at this point?

Mr. Duane Schippers: Every case is going to be unique in terms of how long it's going to take.

If we talk about resources, no law enforcement agency is ever going to be able to tell you that they have every resource they'd like to have, because they'd probably want to take every case forward. They don't have the resources to take every single case forward that comes in the door. They do have to exercise some discretion, and they look at alternative case resolution methods.

Many times in our work a complaint can be resolved by an investigator calling the subject of the complaint and discussing what the misleading advertising issue is. Often that leads to voluntary corrective action. Quite frankly, that's our first preference. We don't want to spend a lot of taxpayer resources prosecuting businesses that are legitimate businesses that just occasionally step offside either because they misinterpret the legislation or because they're trying to be innovative and creative in what they're doing.

But we do take action against false and misleading advertising, and if it's false and misleading, we're going to take action. With the resources we've requested, we are confident that we'll have the resources we need to deal with any additional complaints coming in as a result of our spam complaints.

● (1630)

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

Mr. Van Kesteren.

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

Thank you, guests, for appearing here today.

Some businesses would argue that they should have a right to contact and advertise. I want to know what the difference is between sending some types of spam, which some would argue is advertisement, and junk mail, because many of these addresses are also traded between mailers.

In connection with that, in your opinion, will the provisions aimed at dealing with address harvesting and the unauthorized collection of personal information via unauthorized access to a computer interfere with legitimate practices currently under way?

Madam Denham, could you maybe answer that?

Mr. Carman Baggaley: Let me address the first part of the question about whether this hinders the ability of businesses to engage in legitimate marketing. In some ways, I think using electronic means of communication to do marketing is quite different from, say, direct mail.

One obvious example is if someone is using text messages. Many services impose a cost when you receive a text message. No cost is imposed on me when I receive something in my mailbox.

Another problem with electronic messages is that we've seen this phenomenon of phishing. Sometimes it's very difficult for the individual to figure out if it's really an e-mail from RBC or whether it's simply some organization pretending to be RBC. Also, e-mails can have viruses in them.

There are all kinds of harms that can arise with respect to electronic messages that don't arise with respect to direct mail in particular. So for many of those reasons, and certainly the cost that imposes on businesses, which I think you've heard about, we certainly think the regime that's being created to deal with electronic messages is reasonable.

With respect to the issue of address harvesting, this is a difficult issue. Again, we think what this is intended to deal with is organizations that are collecting e-mail addresses, using what are called dictionary attacks to generate lists of e-mail addresses, and then either using them to send spam or selling them.

We've had some discussions about whether or not it would be necessary to make small adjustments to that provision to deal with some scenarios. We're open to minor adjustments on the address harvesting, particularly to deal with cases where we understand that a search engine, for example, may collect e-mail addresses in order to determine where they're coming from.

When you search on the word “Chelsea”, if you're in England, it's probably the football club. If you search on the word “Chelsea” in the United States, it may be the district of New York. You want to know where they collect e-mail addresses. There may be ways to address some of those problems.

Mr. Dave Van Kesteren: In connection with that, do you feel that the government has struck an appropriate balance between legitimate business and catching the bad guys? I guess that's what we're concerned about more than anything else. Do you foresee any negative implications for legitimate businesses?

Mr. Carman Baggaley: I'll be quite honest. It's very difficult to draw the line between legitimate businesses and illegitimate businesses, and it's very difficult to craft legislation that deals with that. Now, having said that, I think the provisions that allow people to send electronic messages if there's an existing business relationship are one way of addressing that.

I think the other point worth emphasizing is that if you're like me, you're fairly careful about to whom you give your e-mail address. By doing that, I think in many cases you're going to ask why they're asking for it, and you're going to have a pretty good idea of what the person is doing. It wouldn't be that hard to build consent into that process upfront.

● (1635)

The Chair: Thank you very much, Mr. Baggaley and Mr. Van Kesteren.

Monsieur Vincent.

[*Translation*]

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

Mr. Schippers, you referred earlier to a study you did on new resources that you would be needing. Is your study based on your own experience or that of countries that have enacted similar legislation?

Mr. Duane Schippers: We did two things. First, we did a comparative study of the current legislation and the new powers we would have under Bill C-27. We also compared what is going on in the United States, Australia and the United Kingdom.

[*English*]

At the end of the day, in each of those countries, the types of changes made to the competition or consumer protection legislation were very similar, we think, to the types of changes being made here. Their mandates were expanded slightly, but the core focus of their mandate remained false and misleading advertising—not a huge change in the mandate.

Then we looked at our own resources and determined what we'd need to purchase in terms of additional software and other technology equipment to carry out our role, and also what additional people resources we'd need.

That's how we came to determine what our resource requirement would be.

[*Translation*]

Mr. Robert Vincent: Is that study available?

Mr. Duane Schippers: No. They were internal studies. This is not a public study; it is not on our website.

Mr. Robert Vincent: Even if the study is not posted on your website, we can request to receive that study. Based on what you are telling me, you spoke with two or three people, and based on your conversation with those people, things are fine. Yet, you did not carry out any study to determine anything concrete. You are saying that you checked up on the situation in the United States, Australia and the United Kingdom. Comparisons would have been done, letting you know that you would be needing such and such a resource or a given software. You carried out an internal inquiry, which became a study. That is what you are telling me.

Mr. Duane Schippers: Perhaps the word “study” is not the best word to use. We called our colleagues abroad and asked them what they did with respect to their legislation. We made notes, within our organization. That is how the Bureau's employees carried out the study. We did not hire anyone externally to do the study. We used our own resources.

Mr. Robert Vincent: I understand; but without having to hire anyone, notes could have been made, allowing you to tell the government that, based on your information, you would need two or three extra employees and additional software. You could submit that to the government to get the resources and money you need to carry out concrete work on Bill C-27.

[*English*]

Mr. Duane Schippers: We have a group of people in the bureau who look at our resourcing and make those extrapolations as to what the likely impact is going to be and what's likely required. Then there's a whole cabinet process that goes through that.

● (1640)

[*Translation*]

Mr. Robert Vincent: Thank you.

Ms. Denham, you said that you will probably not have to carry out many investigations. However, I remember that there was an investigation to which there was no concrete follow-up. That investigation was on the national do not call list. There was an uproar that was reported in the newspapers because anyone was able to purchase the national do not call list for $35 or $50, and get thousands of names.

Will the same thing happen with the national telecommunications opt-out list, or have you taken measures to make sure that what happened with the do not call list does not happen again?

[*English*]

Mrs. Elizabeth Denham: Well, the do-not-call list, so complaints about the do-not-call list, would have gone to the CRTC in that case. But if your question is whether we anticipate a flood of complaints about address harvesting, for example, I think it might be difficult, in a lot of cases, for individuals to actually know what organization has committed the crime, so to speak, or who's in the wrong there.

So no, we don't expect the same kind of volume of complaints under the ECPA.

The Chair: Thank you very much.

Mr. Wallace.

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

I want to thank our guests for coming this afternoon.

Just so you know where I'm coming from, I've been asking for us to get to line-by-line here to get this legislation through, because I think it's important to get it through. We've been talking about it for a number of years here on the Hill. Things are getting worse instead of better, of course, in that spam world.

I appreciate your comments. We've heard comments from other individuals and organizations about how big the net is. I think we need to start with the big net, to be perfectly frank with you, and then make some changes if required.

I was on a previous committee—Ms. Denham, it's nice to see you again—and we reviewed PIPEDA. It has an automatic review built into it. I think it's five years.

Do you have any comments from your organization as to how you'd feel about a five-year review attached to this piece of legislation?

Mrs. Elizabeth Denham: I think it's very useful to have a review process built into the statute. It is a very good process, especially when you're dealing with legislation as new as anti-spam for Canada.

We had a very thorough and good review process, as you know, in PIPEDA. We're waiting for perhaps some more amendments. We'd like to see some mandatory breach notification coming our way—I'll just slip that in—because I think that's part of this whole world.

I agree that there should be a review process, especially when we all recognize that it's a simple problem, spam, but a difficult fix, a complex fix. I would encourage a review period.

Mr. Mike Wallace: I appreciate that.

To Monsieur Vincent, our next guest in the next hour is from the CRTC. I could be wrong, but to my understanding, that story about the list being available to be bought was actually false and not accurate. I'd like to know more, so if you don't ask the question, I'll be asking the question.

My question now is for the Competition Bureau. Hopefully you're able to answer it.

There is an exception in here for business-to-business communications. Do you as an organization have any issues with that? Most organizations that have come to see us have appreciated that there's a business-to-business exemption.

I'll use the wild example—this doesn't actually happen, and I want that to be on the record—of an insurance company, let's say, that's using spam to bug me about buying insurance from them. I've had no past relationship with them and I've never bought life insurance from them. But they keep sending me e-mails. I'm not happy about that. I can take action if this bill becomes law.

In a previous life, I sold racking systems for servers and monitors. I actually sold to many of the large insurance companies. They have beautiful computer rooms in their basements, with lots of names on them. I was able to put their hardware on a lot of my racks.

Under this legislation, an insurance company would still be able to e-mail me—or I could e-mail them, because they are a customer—any discounts, anything I had, as long as there was a relationship; that's my understanding. But in terms of starting a relationship, have you read anything in here, or could you tell me what you believe this would do, with regard to me trying to start a relationship with, say, a large insurance company that I'm trying to sell something to, from a business-to-business perspective?

● (1645)

Mr. Duane Schippers: I think I'm going to let you ask that question of Mr. von Finckenstein, perhaps, when he comes here.

The reason I say that is that the way the amendments to the Competition Act work, there is no exemption for business-to-business communication. If you engage in false and misleading advertising, it's false and misleading advertising regardless.

Mr. Mike Wallace: It's just the advertising side. Okay.

So your role at the Competition Bureau is that if somebody, through the use of the electronic system, is promoting something that's not accurate, then we could take action on that, through you.

Mr. Duane Schippers: That's exactly right.

Mr. Mike Wallace: Thank you very much.

Those are my questions.

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

Mr. Masse.

Mr. Brian Masse: Mr. Chair, I don't have any further questions.

The Chair: Okay.

Mr. Lake, do you have any further questions?

Mr. Mike Lake: Yes. I have a couple of them.

First, as we're reviewing the legislation and potentially getting ready to go to clause-by-clause eventually, have there been any changes since the legislation has been drafted that you have identified and want to point out now? I'll just give you the opportunity to point out anything that you think you've heard in testimony, or whatever the case may be, where you might say, “You know, that's a legitimate point.”

Perhaps there's a minor tweak or something. It doesn't sound like there are any major ones, or you would have brought them up by now.

Ms. Hedy Kirkby: We've identified a few things to Industry Canada for their consideration. Some are really just technical errors that were made in the final hours of drafting.

Perhaps one matter that we have been discussing with Industry Canada would be worth mentioning. We're permitted to share information, under the amendments that are being made here, with the CRTC and Competition Bureau. An amendment was made to PIPEDA to accommodate that. What wasn't done, and what we believe would be useful, was an expansion of that provision to enable us also to disclose information when we are intervening in a private right of action.

That was an oversight. Without such a provision, we would be prohibited under the confidentiality provisions in PIPEDA from effectively intervening in such a matter. We've brought that to the attention of Industry Canada.

Mr. Mike Lake: Mr. Schippers.

Mr. Duane Schippers: From the Competition Bureau's perspective—and we don't see it as a significant problem at this point—we want the most effective way possible to share information with our international counterparts so that we can take action quickly. Our concern is to make sure there are appropriate safeguards in the use of that information when it's shared, but whatever can be done to facilitate the sharing of information with international enforcement agencies is important in this borderless world of spam.

Mr. Mike Lake: Going back to comments from the last committee meeting, I'll just read a quote from one of the witnesses, who said:

> The bill would literally also prohibit consumers from e-mailing retailers, demanding a refund, asking for support, making a warranty claim within 18 months after purchasing a product.

Ms. Denham, in your interpretation of the bill, does the bill actually do those things? Would it, for example, make it impossible for someone to make a warranty claim 18 months after purchasing a product?

Mrs. Elizabeth Denham: No, I don't see that. I don't see that kind of prohibition. If a consumer needs to contact the retail organization, they can do so.

Again, if somebody purchases an expensive television and they're giving their e-mail address to the company, there's going to be a notice provision there. They're collecting an e-mail address, so again, I don't see the difficulty with warranties and recalls.

● (1650)

Mr. Mike Lake: Okay.

There was also some talk about general updates on computers. We all have this. Windows needs an update and Microsoft just automatically accesses the computer and updates the software. But there was some concern that there would be cases in which there was an urgent need for an update on the computer and, under the provisions of this bill, a company wouldn't be able to actually access the computer to put that urgent update on there.

It seems to me that if there is a need for an outside source to access their computer, and they actually have the means to do that—they know where the IP address is to be able to get in and get onto your computer—there has to be a way that they got that information in the first place. Thus, there would be a mechanism for me to say yes, when there's an urgent situation on my computer, I'd like you to fix it.

Am I misreading that in any way, or is there anything you want to add to that?

Mrs. Elizabeth Denham: I think that might be an unintended consequence of the drafting. I certainly think Canadians expect and want those upgrades on their computers, so I understand that Industry Canada is looking at tweaking the language to make sure that's taken care of.

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

Mr. McTeague.

Hon. Dan McTeague (Pickering—Scarborough East, Lib.): Chair, thank you very much for this.

I thank you, witnesses, for being here today.

It's a real pleasure and a treat to be back on the industry committee. It feels like old times.

As the author of the first anti-spam legislation in 2002-03, I'm really pleased that, several years later, Mr. Chair, we're getting onto this and, more importantly, the lawful access.

I'm going to start to charge a copyright fee for all the ideas that are now being taken by my colleagues.

Mr. Chair, I wanted to ask a question.

Ms. Denham, following up on Ms. Coady's remarks this morning on the collection, the enforcement of a private right, and the purpose of enforcement and the law, it would appear to me that provisions or exceptions have not been made to those two types of actions that have been legally enforced.

How do you reconcile the two? If I have a legal mandate to acquire personal information or collect an address, either by law or by a private right of action, what trumps the other? Which one prevails—your law or the law ordered by a court?

Mrs. Elizabeth Denham: I'm not sure I quite understand it.

Do you mean does PIPEDA trump a private right of action?

Hon. Dan McTeague: I mean the way you've drafted it here in clause 78 of the legislation.

Mr. Carman Baggaley: Let me try to clarify.

Clause 78 is designed to deal with using a computer program to collect e-mail addresses. If I were engaged in a lawsuit against you or any other individual, there would be any number of other mechanisms I would use to get the e-mail address or any other information I needed. I could get a deposition, or we'd work through lawyers. But certainly this idea of a prohibition on being able to collect e-mail addresses using a computer program seems to be overstated, because in many of these situations, again, if I'm dealing with a one-on-one case with another individual, there are other ways to get this information without using a computer program.

Hon. Dan McTeague: Assuming, then, a scenario, we have to look at the probabilities of these things happening. When you put together the legislation, under clause 78, did you take into account in any way, shape, or form the legitimacy of a requirement for public or private enforcement? I think that's really the issue at hand.

You're saying it's overstated. I'm suggesting to you that certainly there is a legitimate concern. If I've been directed by a court to use or have a right to use, other than through consent, where do you draw the line?

Mr. Carman Baggaley: Again, I think I would refer to the fact that, in our view, that is written relatively narrowly. It refers to using a computer program to collect e-mail addresses. Again, if for some reason a law enforcement agency wants to collect 10,000 e-mail addresses from a telecommunications service provider to investigate possible hate e-mails, I don't see anything in this legislation that would prohibit it.

● (1655)

Hon. Dan McTeague: We've talked about similar legislation occurring around the world, and I certainly see us as sort of falling behind in this. This follows as well on Ms. Coady's remarks earlier. I'm not sure we got a satisfactory answer on this. Do you feel that the legislation you've provided here in clause 78, not linked specifically to the word "spam", makes it broader than that of the United States, makes it broader than New Zealand's, and makes it broader than Singapore's? I'm really trying to find the broader purpose of not actually relating it to spam, spelling it out, and defining it.

Mr. Carman Baggaley: Again, we don't think it's overly broad. In fairness, we really haven't had anyone come to us with specific examples of what it would prohibit, or of what is now permissible that would become prohibited under this legislation, so it's difficult for us to respond to that. Again, there are ways to make "minor"—that's the word we use—adjustments to that provision without opening it up completely. That's something that could be considered.

Hon. Dan McTeague: As an observer, again, I'm looking at this from more of a layman's perspective. It would appear that what you have done in reducing some of the exclusions you have in clause 78 for other purposes—not defined as spam—is that you've in fact opened yourself up to some pretty substantial changes in PIPEDA, which were never intended or perhaps not contemplated by the limited nature of that legislation as it was first presented.

Do you not believe that we should perhaps have a separate, stand-alone piece of legislation to introduce these rather substantial changes, whether it's implied consent or explicit consent that's required? It sounds like you're biting off quite a bit more than you can chew and, more importantly, possibly opening us up to the countervailing view that this is far more broad-reaching than it ought to have been.

Mr. Carman Baggaley: Let me first start with a sort of caveat. This is Industry Canada's bill, not the Office of the Privacy Commissioner's bill. We have an interest in a relatively narrow set of provisions in the bill.

Our view is that it's not overly broad. On this issue of spam, one of the difficulties is that it's very difficult to put into legislation when you cross the line between unwanted e-mails and when it suddenly becomes spam. We thought about that. It's just a very difficult thing to try to figure out when you go over that, when you tip the balance.

The Chair: Thank you very much, Mr. Baggaley. Thank you very much, Mr. McTeague.

Thank you to members for their questions and comments. Thank you to our witnesses for their testimony.

We'll suspend for 15 minutes and reconvene at 5:15.

● _____ (Pause) _____

●

● (1710)

The Chair: Welcome to the 30th meeting of the Standing Committee on Industry, Science and Technology. We're here pursuant to an order of reference of Friday, May 8, 2009, concerning Bill C-27.

We have in front of us today three representatives of the Canadian Radio-television and Telecommunications Commission: Mr. von Finckenstein, Mr. Katz, and Mr. Traversy.

Welcome to the three of you.

Mr. von Finckenstein, you now have time to give us your opening remarks.

Mr. Konrad W. von Finckenstein (Chairman, Canadian Radio-television and Telecommunications Commission): Thank you, Mr. Chairman, for the opportunity to meet with the committee to discuss the Electronic Commerce Protection Act.

[*Translation*]

We are here to support Bill C-27 and explain our role, as envisaged in the bill. We are glad that the government has introduced this legislation, which is essential to Canada's growing digital economy. It will also have the added benefit of bringing Canadian law in line with our peers in the G8 who have already enacted similar anti-spam legislation.

As the committee knows, the bill is designed to counter commercial spam and related online problems, such as spyware, malware and phishing. These are problems that undermine confidence in the electronic marketplace.

[*English*]

Under the bill, the main enforcement responsibilities for spam will fall under the responsibility of the CRTC. We will be responsible for investigating violations and ensuring compliance.

[*Translation*]

The Competition Bureau will address false or misleading representations made through electronic messages. The Office of the Privacy Commissioner will address the invasion of privacy stemming from the collection and use of email addresses by computer programs.

[*English*]

The CRTC will be responsible for enforcing three types of violations under the act. First, we will enforce the "no spam" provisions of the act.

The ECPA provides for an “opt-in” regime, whereby people must first consent to receive commercial electronic messages. If there is no express or implied consent, spammers are subject to monetary penalties. Consent will be considered implied under one of two conditions: (a) where there is a business relationship that has been in existence for any time during the last 18 months, or where the recipient has made an inquiry or application within the last six months; and (b) in a non-business relationship where, in the last 18 months, the recipient has made a donation or gift, provided volunteer work, or signed a membership.

Second, the CRTC will prosecute violations involving the alteration of transmission data in an electronic message. Altering transmission data without express consent is prohibited.

Thirdly, the CRTC will enforce the prohibition against installing software or causing it to be installed without express consent. This has been a growing problem, as some spam has been designed to install software into a host computer, and this software in turn broadcasts further spam messages.

The bill provides for tools to permit the CRTC to enforce the act. The CRTC will be able to require telephone companies that provide Internet services to preserve time-sensitive transmission data. We will also be able to require telecom service providers and other institutions to provide documents and reports. Furthermore, there is a provision for searches with a warrant.

The act will be enforced on two separate tracks. The CRTC will have the authority to issue administrative monetary penalties of up to $1 million for an individual and up to $10 million for a business. We will also have the authority to negotiate binding undertakings. The second track involves the right to sue, which will allow individuals and businesses to take civil action through the courts to (a) recover damages for losses suffered and (b) to obtain additional damages for violations of the act.

However, lawsuits under (b) above will not be permitted if the CRTC has already issued a notice of violation or if an undertaking has been agreed upon. Similarly, the CRTC cannot start enforcement action if lawsuits have already been launched under (b) regarding the same violation.

● (1715)

[*Translation*]

One of the most important features of this bill is that it gives each of the federal partners—the CRTC, the Competition Bureau and the Privacy Commissioner—the ability to share information with one another, as well as with foreign partners.

[*English*]

While there is much to commend in Bill C-27, we believe there is room for improvement in two key areas.

[*Translation*]

The first concerns section 27, which provides the right to appeal certain CRTC decisions to the Federal Court of Appeal. We propose amending this section to provide a timeframe for bringing such appeals to the Federal Court, and suggest that 30 days would be sufficient. The wording for this proposed amendment can be found in the appendix to this speech.

[*English*]

Secondly, we would like to propose an amendment to the information-sharing provisions of the bill to strengthen the CRTC's ability to work with the U.S. Federal Trade Commission and other international bodies operating under similar anti-spam legislation.

As it has been drafted, the bill allows the CRTC, the Competition Bureau, or the Office of the Privacy Commissioner to share information with other countries provided there is an international agreement or arrangement. In our view, these provisions fall short of what will be required to effectively counter spam. We know that spammers can be very adept at locating in one jurisdiction and directing spam at another jurisdiction. Living in North America, we can expect that a good deal of spam originates or will originate from our southern neighbours.

In its 2005 report, the task force on spam recognized that international enforcement of spam is essential. It recommended that:

> The federal government, in coordination with the provinces and territories, should conclude and implement cooperative enforcement agreements with other countries. These efforts should include examining and amending existing legislative provisions as required to allow for seamless international cooperative investigative and enforcement action.

We agree that cooperation with other countries, and particularly with the United States, is essential. But clause 60 of the bill allows for cooperation only on the basis of intergovernmental or interagency agreements or arrangements. From my own experience as Commissioner of Competition, I know how difficult it can be to reach such agreements and how time-consuming and complex the process has become. It is essential that once the legislation has been enacted we can move quickly to cooperate with the United States. We can't afford to wait years until there's an international agreement. The process of negotiating the agreement should not be a barrier to working together to counter spam.

In 2006, the United States passed the Safe Web Act. It gives the FTC the authority to conduct investigations on behalf of a foreign agency, such as the CRTC, that is investigating conduct that is also prohibited under laws enforced by the FTC. However, in our view, and based on past experience, the FTC will provide assistance only if the country in question has reciprocal legislation. No such reciprocal provision is found in Bill C-27.

If Bill C-27 were amended so that it would mirror the provisions in the Safe Web Act, such cooperation would not be problematic; it would be automatic, and it would obviate the need for lengthy negotiations of arrangements or agreements.

We have drafted a proposed amendment, numbered 60A. You will find it in the appendix to this speech. Subject to certain safeguards, it would specifically empower the commission to gather information and evidence on behalf of a foreign country with similar reciprocal legislation, i.e., the United States. This assistance would be provided further, through a written request, in cases of alleged civil contraventions of foreign laws regarding conduct that is substantially similar to that prohibited in Canada. The proposed amendment would also allow the CRTC to share that information with the foreign entity in question.

In essence, clause 60A would provide for mutual assistance between Canada and other countries. I would emphasize that this provision would apply only to the gathering and sharing of information. The decision regarding whether to proceed would be entirely up to the CRTC and would depend on whether the foreign agency had agreed to provide reciprocal assistance.

The addition of clause 60A will require minor changes to the wording elsewhere in the bill to ensure consistency. For that purpose, the proposed changes to clauses 15, 17, and 19 are set out in the appendix.

[*Translation*]

In conclusion, both proposed amendments, with respect to the appeal period and cooperating on investigations, are very much in keeping with the spirit of the bill as passed for second reading in the House.

In the absence of section 60A, we believe it will be difficult to work quickly and cooperatively with foreign entities, and in particular the FTC. Without this amendment, the Commission's ability to address spam will be compromised significantly.

[*English*]

Thank you very much.

We will be pleased to answer any questions.

● (1720)

The Chair: Thank you very much, Mr. von Finckenstein.

We'll have about an hour of questions and comments from members of this committee, beginning with Madam Coady.

Ms. Siobhan Coady: Thank you very much.

We certainly appreciate your coming here this afternoon and sharing your expertise with us. This is indeed a very important bill, and it's a long-awaited one. It's very important to Canadian business in particular, but also to Canadians who use the Internet.

Mr. von Finckenstein, I have a couple of questions. First of all, on your proposed amendments, you've addressed one of my concerns with this bill, which is the right to appeal. Thank you for addressing that so comprehensively. I have a couple of questions on that particular change to the right to appeal. You're suggesting that 30 days would be sufficient. Why do you think 30 days is sufficient? Second, do you think there should be any kind of appeal process to the CRTC prior to going to the courts?

Mr. Konrad W. von Finckenstein: We're talking here about the provisions regarding preserving evidence or making reports. First of all, we ask them, but let's say the telephone company in question is not willing to do it. They can ask the CRTC to review it. There's a time period provided and then the CRTC will make the decision. It's very quick. Then, if you're still unhappy, you can go to the Federal Court.

We see no problem with that, but we suggest that it should be 30 days because that's the standard period for appeals to the Federal Court of Appeal. Your decisions from the Competition Bureau, for instance, also have 30 days, etc., so that's the norm. We just felt that it shouldn't be left open-ended. Otherwise, you could come with that after half a year and try to make an appeal.

● (1725)

Ms. Siobhan Coady: I have two other quick questions and only a few moments.

The ECPA would make violation of the provisions subject to administrative monetary penalties of up to $1 million in the case of an individual and $10 million in the case of non-individuals. Now, as you know, these high penalties can be exacted without the right to a trial, and what you're suggesting there is merely a right to representation. Are you saying that what you're suggesting is a balance to that approach?

Mr. Konrad W. von Finckenstein: No, no—

Ms. Siobhan Coady: Would it just be clause 27?

Mr. Konrad W. von Finckenstein: It's just the sections on where you're appealing a decision of the CRTC.

Ms. Siobhan Coady: Did you not consider—

Mr. Konrad W. von Finckenstein: No. Just to understand, you've said a couple of things that are not quite correct. For the administrative monetary penalties and what happens there, there's going to be an investigation by the CRTC. The staff then talks to a commissioner and asks if it is legitimate and so grave or so persistent that we should proceed by way of administrative penalty. The commissioner then says yes or no, and we send it to the alleged violator, saying that we have investigated and here is the evidence we have. We say that we feel they are in violation and their violation requires a fine of *x* dollars, and we ask them to please send their comments.

They then send their comments. Then, in effect, the accusations by the staff of the CRTC and the defence by the party are put to a panel of three commissioners of the CRTC who have up to that point not been involved and will make a decision. That's the procedure. The appeal to the court of appeal is on any decision of the CRTC, including the AMP decision.

Ms. Siobhan Coady: Thank you.

I want to move now to “Rules About Contraventions”, clause 52, which states:

> An officer, director, agent or mandatary of a corporation that commits a contravention of any of sections 6 to 9 is a party to and liable for the contravention if they directed, authorized, assented to, acquiesced in or participated in the commission of the contravention, whether or not the corporation is proceeded against.

My concern here is that the liability will extend to employers, officers, directors, or agents of the company, and that we may be, through that clause, discouraging individuals from accepting management roles in Canadian business. I'm wondering about your thoughts on that. Am I interpreting that correctly?

Mr. Konrad W. von Finckenstein: Your interpretation is correct in that one of the consequences that follows that you're.... I mean, it's unlikely that if you're a director or officer of a corporation you would act with intent to break the law, which is what you have to do here. I'm sure your employer doesn't ask you to do that.

It's no different from any other law, all sorts of other laws, where you can go after the officer or the corporation or both. Normally we only go after the corporation, because the corporation will take the necessary disciplinary action to make sure that its individuals obey the law, but you have the option to go after both. I don't see that this will in any way discourage people from working in Canada or assuming responsibility.

Ms. Siobhan Coady: Thank you.

Do you have any questions?

Hon. Dan McTeague: I'd take more than one minute. It would take several minutes.

Ms. Siobhan Coady: Okay, I'm done.

Thank you very much.

The Chair: Thank you, Madame Coady.

Monsieur Bouchard.

[*Translation*]

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

I would also like to thank the representatives from the CRTC for appearing before us. My first question is for any one of you three.

You talked about cooperative agreements with the provinces, the G8 countries and organizations outside Canada. You also mentioned that there would be some exchanges between the Office of the Privacy Commissioner, the Competition Bureau and the CRTC. Will each of your organizations reach its own agreements with each province and country, or has any thought been given to something simpler, some type of cooperation or exchange? Your three organizations are covered by the same bill and will have to adopt protocols. What steps do you intend to take? Will you be coordinating your efforts or will the three organizations act independently?

● (1730)

Mr. Konrad W. von Finckenstein: First of all, the Competition Bureau, the Office of the Privacy Commissioner and the Canadian Radio-television and Telecommunications Commission are three federal agencies with confidentiality obligations. They cannot swap information unless permitted to do so by law. They are not compelled, but they may share information to facilitate things for another organization, consumers or complainants. We can work in collaboration when the opportunity arises.

Secondly, clause 60 of the bill under review states that we can swap information and even do research for other foreign organizations, providing that there is an international arrangement. This is a good thing, but it is complicated. I have been a competition commissioner, and I know that it takes a great deal of time to do this. We have to get other organizations and departments to participate, there are always political considerations, and so forth.

I have taken a look at what the Americans have done on this issue. They felt that it was essential to be able to swap information with another country and do research for a foreign organization that has authority and legislative provisions similar to theirs. We are suggesting this approach because it is quick. Most of the spam comes from the United States. It is absolutely crucial that, at the outset, Canada and the United States be able to cooperate and help each other out. It will take several years before an international arrangement can be negotiated and, meanwhile, we will not be able to do anything about these emails coming from the United States.

Mr. Robert Bouchard: It is good to hear you say that you will be cooperating with institutions outside Canada, but I would like to ask you my question again. Will the information gathered by the Office of the Privacy Commissioner, the Competition Bureau or the CRTC be mutually accessible, so that there will be no duplication of effort? I am not sure whether there will be any real coordination.

Mr. Konrad W. von Finckenstein: As far as this bill is concerned, we have most of the responsibility. We are responsible for prosecutions in the case of an offence. If someone is sending spam, it may contain misleading advertising and the Competition Bureau would need this. Rather than start its own enquiry, the Bureau may inform us that it has received complaints about this individual. If the Bureau is aware of the fact that we are in the process of prosecuting the individual for sending spam, it can seek our permission to obtain the information we have in order to determine whether or not there are grounds for a charge of misleading advertising. That is one example.

In most cases, there will be separate and targeted legal proceedings for specific offences. Nevertheless, in cases where there are two aspects to the offence, we may share the information.

Mr. Robert Bouchard: Is the CRTC responsible for coordination? Will there be some small organization that coordinates the three agencies? Indeed, even though three agencies are involved, someone may not be responsible for this. Has any thought been given to leadership or coordination between the three institutions?

● (1735)

Mr. Konrad W. von Finckenstein: No, this does not exist, and I do not believe that it will be necessary. Each of us has a specific task, which is quite different from the tasks of the other two. Should there be a divergence or an overlap...

Mr. Robert Bouchard: Do you mean a conflict?

Mr. Konrad W. von Finckenstein: Not a conflict, but something that concerns both of us. We can share, however, in the majority...

Mr. Robert Bouchard: So you mean overlap?

Mr. Konrad W. von Finckenstein: Indeed, overlap. Most of the time, this is not the case. I believe that there are very few instances where the competition commissioner or the privacy commissioner will get involved in violations. We get involved in the vast majority of such cases.

The Chair: Thank you, Mr. Bouchard. Thank you, Mr. von Finckenstein.

[*English*]

Mr. Lake.

Mr. Mike Lake: I'm going to start with a look at clause 20, which talks about violations. Subclause 20(3) says:

> The following factors must be taken into account when determining the amount of a penalty:

Then it goes through a list of the different things that have to be taken into account.

In the previous meeting, there was some concern raised by a couple of different witnesses about the amounts involved in the administrative monetary penalties—i.e., $1 million for individuals, $10 million for businesses. The concern was that there would be some minor violation of the act and a company would be subject to a fine of $10 million. For an individual, it would be $1 million for a minor violation.

As I read clause 20, though, it seems pretty clear that there are measures within the bill to ensure that this won't be the case. Maybe you could comment on the use of AMPs in this way.

Mr. Konrad W. von Finckenstein: First of all, it's "up to" $1 million or $10 million. It could be $10, $100, $1,000, or whatever is appropriate.

Secondly, we, like every enforcement agency, have a compliance compendium. You start off by educating people. You warn them, you try to get them to comply, you try to educate them. Then, if there is resistance or a wilful breach, you can fine them.

When you do fine them, you take into account the gravity of the action taken. Was it deliberate or was it unintentional? Was it repetitive? What was the cost damage? When you impose a fine, you take into account both aspects—the deterrence aspect, in that it should be a lesson to this person and others not to do it again, and also the effect it will have. You don't want to put somebody out of business. You just want to make sure they get a meaningful lesson and won't do it again.

Now, if it's somebody who is just deliberately, consistently, and wilfully breaching, etc., obviously you may go close to the maximum or to the maximum. It depends; you make an assessment of the circumstances.

Mr. Mike Lake: Right. Thank you.

Just following up on the Bloc's questions, I want to talk a little bit about the three agencies involved in the enforcement.

What is the justification behind having the three agencies enforce the proposed new law? Maybe you could elaborate a little bit more on the role for each. You say there's not going to be overlap, but how do we make sure that the three agencies cover off everything we want to cover off?

Mr. Konrad W. von Finckenstein: The act basically says it's an opt-in scheme. I may not send you an e-mail unless I have your consent, implicit or implied. That is a key provision, and it falls squarely into the realm of the competence of the CRTC. We enforce it. We decide whether or not there was consent. If there was no consent, we take remedial action.

The act also addresses two subsidiary offences. Not only could spam bother you with e-mails that you don't want, it could also send you misleading information that you act on to your detriment. To the extent that happens, the competition commissioner is specifically empowered to deal with the misleading advertising aspect of spam. As I say, I think they really could do it right now, because they have a ban on misleading advertising at any time, in any form. The act specifically means they can also do it for spam.

So is spam purely the jurisdiction of the CRTC? No, it's not. If you use spam for misleading advertising purposes, you also have to account for it to the competition commissioner.

It's the same thing if you use spam and address lists to somehow do something that violates the privacy provision of either the Privacy Act or PIPEDA. The Privacy Commissioner can come after you then.

So that's the scheme.

● (1740)

Mr. Mike Lake: All right.

You talked a little bit about international cooperation. What experience does the CRTC have in cooperating with communications authorities in other countries under the Telecommunications Act and the Broadcasting Act?

Mr. Konrad W. von Finckenstein: We have very good cooperation. We exchange views and information. But everybody is bound by the provisions of the statute and by the extent to which the statute allows you to exchange information or not.

I'm particularly concerned with the United States. For obvious reasons, it's the most important partner for us. My experience is that if you have legislation that basically mirrors the U.S. legislation, it works very well. They know it and understand it and so on. So if you ask that this be subject to international agreement, as set out here, you're going to wait an awfully long time. You're going to get the State Department and the justice and other agencies involved. It would be the same on our side as well. There would always be political overrides for particular situations.

Doing an international agreement is not so simple and straightforward, and here you want to have something quick. If there is spam that comes out of Utah, I want to be able to tell the FTC, "Listen, there's someone in Utah who systematically spams Canada. Get me the information so I can prosecute them."

It's the same thing for them. If somebody in Manitoba spams into the States, I'll investigate. If I have the information, I want to have the ability to give it to them.

That's what the amendment that we put forward allows us to do.

Mr. Mike Lake: You've talked about the legislation that other countries have. How do the information- and evidence-sharing provisions in this bill compare with the legislation and similar measures in other countries—for example, Australia?

Mr. Konrad W. von Finckenstein: I know that the Australian legislation is largely a model for ours and has the same opt-in provisions, etc. I am not acquainted with the details of the information, but they don't have the problem we have: they don't live next door to the biggest economic power in the world with essentially an invisible border.

Mr. Mike Lake: Obviously we're in an age when the digital world is becoming more and more important for us from the innovation side of things. As we move forward, business and personal communications will become the frontier. Well, they are the frontier, and will be even more so.

How important is this legislation in moving us forward in this digital age?

Mr. Konrad W. von Finckenstein: I think it's very important because, as you mentioned, we are living in the age of digital revolution. Our economy is more driven by information—getting information, timely information, using it, and employing it is necessary and can give you great competitive advantages. If the system, however, gets corrupted by spam or phishing or people installing software on your computer so that it becomes unreliable, it can have a major negative impact.

When we first built railroads, we brought in all sorts of rail acts in order to ensure where railways could go and that they would have rights of way. You couldn't interrupt the signals, etc., because having decent railway connection was the main driver of the economy of the country and nothing should interfere with it. Think of that and transfer that to the Internet. You really want to make sure that you have a fast, efficient, reliable Internet that doesn't get monkeyed around by people who do so for whatever motives drive them. They're not economic motives.

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

Thank you, Mr. von Finckenstein.

Mr. Masse.

Mr. Brian Masse: Chair, I thank you for being here. The first question I have is with regard to prohibitions, and the second is with regard to the non-business relationships. Specifically, it says that "in the last 18 months, the recipient has made a donation or gift, provided volunteer work or signed a membership".

What I'm a little bit worried about are things like sports or not-for-profit or world issue discussion groups. Say, for example, you were just a recipient of information and articles over a period of time even beyond 18 months. If somebody were actually doing that, and you were receiving that.... For example, I worked for persons with disabilities before getting here, and I was just receiving information. I liked getting that information, but I'm not volunteering at the organization. I'm not a member of the organization, but I like to keep up to speed on it. Would they have to send out a consent form to be signed, or since I had regularly received that information in the past, would I be able to keep doing so? Are they actually going to have to bring another endeavour?

Once again, I'm worried about those who do informal sports discussions and the exchanges on civil society information and other types of news-sharing that go across personal lists that people have already assembled.

● (1745)

Mr. Konrad W. von Finckenstein: If you worked for them and performed for them, obviously you support that organization; you're interested in it. That serves the equivalent of having a formal or personal relationship. You can receive that and everything. If for some reason you don't like it anymore, etc., there has to be an unsubscribe provision; you can click on that and it will stop. You're protected. But because you were involved, we assume that you supported that organization and you want to continue to receive information. Under the legislation, they're allowed to continue to send you those things.

Mr. Brian Masse: The problem would be if say, for example, you routinely said get me off this list and they refused to do so. You could make a complaint, but until that time, those not-for-profits and other organizations continue to send out that information until there is someone saying that to them.

Mr. Konrad W. von Finckenstein: The act deals with commercial e-mails. What you're describing is a volunteer charitable organization, I assume.

Mr. Brian Masse: Yes. I mean non-business, and even things like informal discussion groups.

Mr. Konrad W. von Finckenstein: Go ahead, Len. Why don't you answer?

Mr. Len Katz (Vice-Chairman, Telecommunications, Canadian Radio-television and Telecommunications Commission): The proposed act basically says volunteer work performed by persons—which is what you're referring to in paragraph 10(6)(b)—will continue on for 18 months.

Mr. Brian Masse: Can it go past that? If I'm just receiving information about that, if I am not volunteering or I haven't signed a membership or done any of those things, but I like getting information from either a formal or an informal group, will they then have to build in a process to have a sign-up form, or can that activity continue until somebody says no and asks to get out of that?

Mr. Konrad W. von Finckenstein: This is there to qualify whether people can send it to you or not. Once they qualify, they are there until such time as you tell them not to send anymore.

Mr. Brian Masse: If this is happening right now, does that qualify you? Are you then okay? Are they going to have to go back to all those people they are in informal discussions with and have them sign on to the form?

Mr. Konrad W. von Finckenstein: If right now you are receiving messages from them because you were involved with them, let's say, two years ago, then it seems to me that yes, they would qualify. If you don't want it, you push the unsubscribe button and you won't get anymore.

Mr. Brian Masse: There may not be an unsubscribe button on some of this information.

Mr. Konrad W. von Finckenstein: They must have it. After this act comes in, they have to put on an unsubscribe button.

Mr. Brian Masse: This is one of the problems I want to research, because those organizations will then have to spend money to have programming done to send out to their list and they will also have to administer it.

Mr. John Traversy (Executive Director, Telecommunications, Canadian Radio-television and Telecommunications Commission): Perhaps I can help.

As the chair mentioned earlier, the act actually applies to commercial unsolicited e-mails that are applied. I think the e-mails you're talking about are of a non-commercial nature so they would not be captured by this act to begin with. If the organization was sending out e-mails and it was trying to solicit or sell a product, then it would come under the realm of the act. But if the organization is just sending out information that someone was used to receiving on the activities of that organization, that is not covered to start with under the legislation. The organization could continue to do that.

Mr. Brian Masse: I thought it was under the non-business relationship, as you were saying.

Mr. John Traversy: The non-business relationship is in fact if they wanted to try to solicit or do commercial activity.

Mr. Brian Masse: Okay, that's very helpful.

I'm surprised this hasn't been raised, but in your conclusion, you talk about your amendments and you conclude with:

> Without this amendment the Commission's ability to address spam will be compromised significantly.

You're saying if you don't get this amendment, the legislation will be seriously compromised. You might want to expand upon that.

Also, if you are going to be doing work with the FCC, what information would you be sharing with it during an investigation? An investigation doesn't mean that someone is guilty; it means that someone is being investigated. I would like to know how we would protect people's personal privacy, especially given that the American Patriot Act is something we can't control and exposes Canadians to loss of public information when it enters into the U.S. stream.

● (1750)

Mr. Konrad W. von Finckenstein: There are several points.

First of all, I want to make sure it has maximum efficiency. We live in North America. We have an integrated economy. That's a fact. We have to deal with it. That's why I want to be able to exchange this information across the border.

Second, with respect to the information that we exchange specifically, we don't have to do it, we just have the power to do it. Nobody can force us to do it. If the FTC asked us, we would look at it. We obviously would check to make sure that it fell within the act. If it did, we would do the investigation. If we found there was something that potentially was in violation, we would give it to them. They could only use it for the purposes for which we sent it, which would be with respect to a civic penalty, nothing else. They could not use it for anything else. That's the provision under which we would give it to them.

Mr. Brian Masse: The problem you face under the Patriot Act is that a couple of different departments can access that information and they're not allowed to tell you that. The FCC would not be able to disclose that the information was being taken from them because that actually would violate the Patriot Act.

Mr. Konrad W. von Finckenstein: You're now making allegations about the U.S. legislation. You may very well be right; I am not an expert on U.S. legislation. This is given by us pursuant to the legislation. The legislation makes it quite clear that it can be used for this purpose and for this purpose alone.

Mr. Brian Masse: That's one thing I'd ask the researcher to follow up, Mr. Chair, with regard to the sharing of information with the FCC and whether it's vulnerable to the Patriot Act and how it would be accessed.

The Chair: Yes, we'll get the analyst to do that.

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

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

Thank you, Mr. von Finckenstein.

Mr. McTeague.

Hon. Dan McTeague: Commissioner, it's a pleasure to have you here before this committee. I can say with some certainty that your role as former competition commissioner was one that saw a number of changes certainly in my time. I'd like to think that the changes we saw in Bill C-10 were the result of your good work and efforts over the past few years. Congratulations to you. I just realized that 10 years of fighting for this and debates back and forth was all done in one fell swoop without a single debate on it in the House of Commons. I was quite amazed at that, even though there are a lot of things in there that I agree with.

Commissioner, you have suggested something that requires a more fulsome explanation. With this bill, we are giving Canadians the impression that by looking after our own mess in our own backyard we are going to suddenly end spamming in Canada. In 2005 the task force recognized that the amount of spamming in Canada is very limited and the effect on Canadians is rather limited. Much of it does come from international sources. Your second recommendation is music to my ears and very much follows with the observation of the task force. I will read it into the record:

> The actions that we take within Canada to reduce the amount of spam will only have a limited effect on the amount of spam arriving in Canadians' email boxes unless these actions are complemented and reinforced by strong, effective international cooperative actions against spammers.

Based on that, sir, not only from the bilateral perspective, but you've suggested that you would be working with the CRTC, the FTC, as well as with the FCC. Who, in your view, would be the lead in coordinating the effort of ensuring that spammers who went to other jurisdictions, not just between Canada and the United States, but...for instance, as I was discussing with my colleague, Mr. Rota, earlier, what if they all wound up in São Tomé?

What reasonable objectives can be achieved in the short term? You've talked about problems of agreements and collaboration and corroboration. How realistic is it that if we provide this legislation, we would stop the spamming in Canada? Also, how likely is it that we would be successful in stopping jurisdictions that have no enforcement responsibilities or any type of agreement in order to put an end to this once and for all?

Mr. Konrad W. von Finckenstein: I think you have to look at it in context. You're talking about commercial spamming, right?

Hon. Dan McTeague: That's correct.

Mr. Konrad W. von Finckenstein: Why do they do that? It's in order to sell something. In order for them to sell something, it has to be something that people want to buy. If you're in São Tomé, as you suggest, in spam, and if you provide for delivery from Canada, we can go after the people on whose behalf it is done. If you want to ship it from São Tomé, there are very few products that are worthwhile shipping from there. In the end, on spamming and the business case, it is really primarily if you're located in Canada and the U.S. That's why I'm so focused on the U.S. That's why I want to have such an agreement with them.

We are not going to eliminate spamming. There's no question about it. As for the letters you get from Nigerians offering you $20 million if you give them a bank account number or something like that, I can't do anything about them because they have no assets and Nigeria has no legislation.

But on the commercial spamming, if people offer you a product you don't want, we can deal with it. We're going to deal with people who try to put stuff on your computer without you knowing it, or the phishing, etc. I think by far the largest source of all of this is in our country or the country to the south, and that we will be able to deal with.

● (1755)

Hon. Dan McTeague: Thank you.

Are you concerned with any parts of the legislation that might be construed as overly broad? My colleague, Ms. Coady, had earlier referred to this.

First of all, on your position on administrative monetary penalties, if they go back to general revenue, how does that assist in targeting finances to the various three agencies that could be involved? Would there not be an understanding, or at least an attempt, to ensure that AMPs go directly to certain departments involved with combatting spam? Would you see something like this as practical?

Mr. Konrad W. von Finckenstein: Not at all. We never have had that, and we never will, because it gives the agencies the wrong incentive. It basically suggests that the more you convict, the more money you're going to have, and that's wrong. You want to make sure that the person who has the power acts objectively in view of the result to be obtained and this has absolutely no direct effect—

Hon. Dan McTeague: How about the party affected?

Mr. Konrad W. von Finckenstein: Well, the party affected can themselves sue. As I mentioned in my opening remarks, there is a private right of action. If you've suffered and you sue, whatever you recover is yours. But you have to prove the damages, of course.

Hon. Dan McTeague: Yes, beyond a doubt, and this is my point, which I think Ms. Coady has made, given that these high penalties can be exacted. As for the penalties that are required here in the form of an AMP, which are up to $1 million in the case of an individual or $10 million in the case of a non-individual, they tend to be without any right of trial.

I know there are concerns about the *ex parte* type of information being drawn without the person being present. There's merely a right to make representation, and a conviction would be entered on proof of only a balance of probabilities. Are you concerned about that given the concerns you just raised about the ability to do these things based on evidence of private right of action? In your experience, do you not think this is overreach?

Mr. Konrad W. von Finckenstein: No. First of all, it's “up to”, right? As I mentioned, really, like any other enforcement agency, you have a continuum of enforcement, and you go to the maximum only in the most egregious cases where you really want to set an example.

Secondly, the way the process works is the examination by one part of the organization and then a decision to proceed with actually a levying of an AMP, of suggesting an AMP. One of my colleagues—actually, it's Mr. Katz here—will make that initial decision. The other parties can then make representations saying that's inappropriate, and that either the facts are wrong or the amount is wrong, etc. Then we will send it to a panel of three commissioners who, until that point in time, know nothing about it and will look at it totally objectively.

Essentially, they hear the accusation and they hear the defence, and they decide. If they decide to levy an administrative monetary penalty, you have the right to appeal to a Federal Court of Appeal. The Federal Court of Appeal will set us straight if we get it wrong.

The Chair: Thank you, Mr. von Finckenstein.

Thank you, Mr. McTeague.

Mr. Wallace.

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

Thank you, gentlemen, for joining us on this topic on what is now this evening. I have only a couple of questions. My one comment, though, based on what was just said, is that I can guarantee you we won't eliminate any spam if we don't get this legislation passed. That's an absolute guarantee. We cannot often guarantee too much, but that we can.

There are a couple of clarifications and then an example that I used before with the Competition Bureau. I just want to be sure I understand the ramifications.

First of all, on the first recommendation in terms of an amendment, you talk about the 30-day issue. I just want to be clear. You have that in other legislation and other requirements. That 30 days is a sort of standard that you would normally work by. Is that correct?

Mr. Konrad W. von Finckenstein: That's correct. It's an appeal. Where there is an appeal from an administrative tribunal to the Federal Court of Appeal, the standard is 30 days.

Mr. Mike Wallace: And you have that in other legislation?

Mr. Konrad W. von Finckenstein: Absolutely.

Mr. Mike Wallace: I just want to be clear.

I'm not as clear about the next one, your second recommendation. According to my reading of the legislation, it actually says—and I think you even say in your opening statement—that as drafted it allows "the Commissioner to share information with other countries provided there is an international...". Your issue is that you don't want to take that extra step of having an international agreement with another country, including the United States. Is that basically what the issue is?

● (1800)

Mr. Konrad W. von Finckenstein: That's one.

The other one is my experience with the U.S. enforcement agencies. When they see a piece of legislation in another country that mirrors their own, and they understand how it works, they have no problem cooperating. If it is different or if it's pursuant to an agreement, then they're worried themselves about exposure in the States to lawsuits, etc., and therefore the default course of action is not to cooperate.

Mr. Mike Wallace: You hit on the next point I had. Even in your statement you talk about mirroring the Safe Web Act that's south of the border, but you're not making any recommendations here—not that I'm reading anyway—to say that this act needs to change to mirror the Safe Web Act.

Mr. Konrad W. von Finckenstein: No, I am not saying that. I am just saying—

Mr. Mike Wallace: But it says here—

Mr. Konrad W. von Finckenstein: Well, I could also say that about other provisions we're not talking about. I'm just saying here's the one for investigating and sharing information.

Mr. Mike Wallace: Just to finish that off, you're not providing this to us today for the first time. I'm assuming you've introduced that to the industry bureaucracy through the process.

Mr. Konrad W. von Finckenstein: I obviously told them I was going to do it. I have no power to introduce amendments. I can only suggest them to one of you, or when somebody else—

Mr. Mike Wallace: Is this the first time you're suggesting them in public or did you suggest them—

Mr. Konrad W. von Finckenstein: This is the first time I have had an opportunity to comment in public. You have invited me, and I'm taking the opportunity to comment.

Mr. Mike Wallace: I didn't know if you were part of the process beforehand. That's fine.

Mr. Konrad W. von Finckenstein: Don't get me wrong. When the government drafted this act, obviously there was consultation with us and others, and they wanted—

Mr. Mike Wallace: Thank you very much.

The final question I have is on the section that deals with an exception for business to business in here. I forget which number it is. I think it's 10(a) or 10(6), or something like that. I would just like to understand and to have your interpretation of it.

A large life insurance company—and this didn't happen, I'm just using this as an example—e-mails me about selling me life insurance, but I have no relationship with them whatsoever and never have had. I'm not interested in life insurance from them. I would consider that unsolicited commercial e-mail to me, which I could take action on based on what I'm reading. But I'm also in the business of selling racking systems for their computer room. So I contact them through their IT department because I want to try to sell them this equipment—it's not false advertising but actual advertising—that they might need to solve their problem of space.

In your view, is that not an e-mail that would be legal in the sense that it's business to business? Under this act, is that a legal e-mail from me or not?

Mr. Konrad W. von Finckenstein: Would you be an independent entrepreneur?

Mr. Mike Wallace: Yes, it's my company. We'll call it L.M. Wallace Racking Systems for now.

Mr. Konrad W. von Finckenstein: Then if it's commerce between L.M. Wallace Racking Systems and the life insurance company, it's a commercial activity.

Mr. Mike Wallace: And that is exempt in this act, is that not correct?

Mr. Konrad W. von Finckenstein: Yes.

Mr. Mike Wallace: Those are all of my questions.

Thank you very much.

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

[*Translation*]

Mr. Vincent, the floor is yours.

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

I would like to congratulate you, Mr. von Finckenstein, and your organization. Indeed, the amendment that you tabled does in fact reflect one of my concerns. I know that this bill is not 100% perfect. Indeed, other witnesses have told us that there are often affiliated programs, that it was possible to obtain lists, in particular, and to go through countries that were not covered by this type of legislation. The problem is that an organization here can forward information to other countries, as is done in the case of the Indian telephone system. These people could therefore go through another country in order to spread advertising.

You said that these products could be delivered to Canada by a foreign company responsible for the distribution and advertising from Canada. With this amendment, in North America, we are going to cover all of that. Of course, it would have been preferable to have had an international agreement, but this is a good start.

I would now like to refer you to clauses 6(4)(a) and 6(4)(b) of the bill, which read as follows:

> (a) an electronic message is considered to have been sent once its transmission has been initiated; and
>
> (b) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination.

Going back to the scenario given by Mr. Wallace, let's suppose that I have my own home business and that my son uses the electronic address list found in my computer in order to sell chocolate for his school. What would happen? From what I can gather, I would be responsible for my computer and individuals under the law. Would there be any repercussions?

● (1805)

Mr. Konrad W. von Finckenstein: Of course. In this type of case, the responsibility falls on your shoulders. If your son were engaged in this type of thing, there could be some complaints. We would have to initiate an investigation, and you would have to describe the situation. We would explain how the law works in these matters, and we would tell you to monitor your son. However, if the problem occurred again, we would have to take requisite action.

But it looks here as though we are talking about an unplanned act, an accident. In such a situation, your son would not have been aware of the provisions of the law. You would simply have to establish a system in order to protect your data.

Mr. Robert Vincent: But the legislation is very clear on that issue. I could be fined. Under the pretext that ignorance of the law is no excuse, I could be told that I should have protected my computer, but that I did not do so, and as a result, the legislation will be enforced.

Mr. Konrad W. von Finckenstein: All legislation includes a discretionary aspect. Even crossing the street on a red light or jaywalking constitutes a crime, but in such cases, police officers usually just warn pedestrians that they cannot cross the street on a red light. The same thing applies here. For such trivial situations, we do not have the time to prosecute.

Mr. Robert Vincent: Have you asked for any additional human and financial resources in order to administer this new act?

Mr. Konrad W. von Finckenstein: We made it clear to the department and to Treasury Board that the administration of this act was not part of our mandate as a regulatory agency for the telecommunications system. In order to administer this act, we will need general funding. We cannot be funded by the telephone companies. The department agrees. If this legislation is adopted, we are going to be given the required funding in order to administer it.

Mr. Robert Vincent: I would like you to talk about the opt-out list. I have also raised this matter with all the witnesses. Will it be possible to more adequately protect the numbers on this list as compared with the telephone list? There has been a lot of abuse, particularly by people who have purchased the telephone lists for the purpose of telemarketing.

Mr. Konrad W. von Finckenstein: Thank you for bringing this matter up, because this is completely false. It is a myth. There is no evidence that telemarketers purchased the list for the purpose of telemarketing. I do not see why they would have done this. This is a list of people who do not want to be called. If you were a telemarketer, why would you buy this list? Obviously, you would not make a single sale. So why buy it? Why waste the money?

Secondly, I read the same thing in the newspaper, but there was never any evidence that a telemarketer, either nationally or internationally, purchased the list in order to call these people. There are some doubts about the fact that there have been violations, and we are in a process of doing an investigation, but to say that someone purchased the list for a perverse reason is a myth. I do not know where this comes from, but it is false. Nevertheless, we have taken additional measures in order to safeguard the list.

Mr. Traversy will explain what we are doing.

● (1810)

Mr. Robert Vincent: Further to the editorials and articles that appeared in the newspapers on this subject, consumers were worried. Television and radio reporters described how this list could be obtained. So the consumers who cannot be here but who are viewing the work of our committee this evening may understand, but for the others who are not watching, who are not listening to us, they may still believe that there is somewhat of a problem with these lists.

The Chair: Thank you, Mr. Vincent.

Please be brief, Mr. Traversy.

[*English*]

Mr. John Traversy: Perhaps I could just add a couple of points to what the chair has mentioned.

First of all, we completed a manual review of all parties who downloaded the list. It revealed that there were only two downloads that were not made by identified telemarketers—to get back to your question of whether there's been abuse of the list—and, coincidentally, in the press there were two public statements of reporters who had downloaded the list using false information.

So our own review indicated—we did an audit—that in fact the list has been downloaded only by telemarketers who correctly identified themselves.

I have a couple of other points, if I can continue on.

The Chair: Just briefly.

Mr. John Traversy: Yes, briefly.

In spite of this evidence, in order to ensure that Canadians have confidence in the list, we have developed a process with the list operator—this will improve on the existing measures—to verify the identity of all individuals or telemarketers before they are allowed to download that list.

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

Mr. Lake.

Mr. Mike Lake: I'll just follow up on that, because this is about the third or fourth time this list has come up in regard to this legislation. Of course, this is different legislation. This is an opt-in system. The only list is of those people who opt in for services from a company. The only organization that has that list is the company that those people opted in with. So it's not even an issue in this legislation anyway.

I want to go back to this proposed amendment that you've put forward. Just out of curiosity, in terms of the discussion you would have had with Industry, what feedback did you get?

Mr. Konrad W. von Finckenstein: “Discussion” is a big word. I told them, “Look, you need this and we need this”, because there had to be a requirement in the act to instantly work with the FTC. They pointed me to the provision regarding it and said they'd addressed it. I told them, “Yes, but not in the way that I think is proper”, and they said, “If you want to put something forward, go ahead”.

So they didn't say yes or no, but I reminded them that the minister, when he appeared before you, suggested that he was open to constructive amendments. I think this falls in the category of constructive amendments. It's a good act; this makes it slightly better.

Mr. Mike Lake: Right.

Actually, I have to say that I appreciate it when any witness who comes forward actually puts forward or suggests an amendment in writing. It's always appreciated. It makes it a lot easier to wade through.

In regard to the suggested amendment, I would point out that in the bill, clause 60, which is being discussed, uses the word “arrangement” rather than the word “agreement”. I think it does so intentionally. It's less formal than the word “agreement”, which would intimate all sorts of formalities and cause some of the concern that you would have. The bill uses the word “arrangement” because it's by definition less formal and allows, to my understanding, the CRTC, the Competition Bureau, and the Privacy Commissioner's office to enter into bilateral arrangements with their counterparts and not necessarily require the formality that you're concerned about.

Maybe you could respond to that.

Mr. Konrad W. von Finckenstein: The arrangement, then, obviously could encompass an exchange of letters or something. But also, as I mentioned to one other questioner—I don't know which one—I am worried about the attitude of the user-enforcer. They have legislation that says you can enter provided there is a reciprocal provision in the other country's legislation. We don't have it explicitly.

If I go to them and say here's my act, section 60A mirrors yours, it's reciprocal, so let's cooperate, there's no problem. If it doesn't, and we want to do an exchange over there, then they always worry about what's happening on their end. Are they within the focus of their legislation, or are they possibly exposed to people saying they are acting outside their scope? Are they divulging information that they shouldn't, or is this arrangement not sufficient, or not strong enough, because they're not speaking about the arrangements that we are?

Therefore, to overcome this, to put it all aside, we have to know how we both work. They want to see some legislation and then we'll feel free to operate and cooperate. Then we will have an exchange of information and we can both fight spam on both sides of the border. That's the reality we face, and that's why I'm suggesting here to put in section 60A. It will do the trick and we can work cooperatively right off the bat.

● (1815)

Mr. Mike Lake: I'll take a closer look at that after we get through the meeting and work on my thinking around that, but I just want to ask the question, does having the word “arrangement” versus the word “agreement” in clause 60 as it stands right now lend more flexibility, in your view, to at least doing the things that you would need to do under this act better than if it were confining you to specific agreements?

Mr. Konrad W. von Finckenstein: Oh, absolutely. The word “arrangement” adds an element of flexibility, but I don't think it's sufficient for the reasons I just mentioned.

Mr. Mike Lake: Okay. Thank you very much.

The Chair: Thank you, Mr. Lake.

Mr. McTeague.

Hon. Dan McTeague: Commissioner, I'm not what I consider an expert in Internet technology, but I do know there are some basics involved with receiving information, with applets that are sent to me to help me view something or that I may ask for and that basically make the system work. I wonder if you and the commission have given any thought, for instance, to access to YouTube.

I know that when I view something, it's possible that my colleague may have done something in that, whatever that may be, and what you will find is that a code would be embedded and stored in the computer's memory. Obviously, I didn't seek the consent, nor did YouTube have to provide me or furnish me the consent. Do you see this as a problem with respect to how modern applications of the Internet can be used? Might this in fact have the unintended effect of preventing it or making it technically impossible, if not commercially impossible, to do this?

Mr. Konrad W. von Finckenstein: No. I don't want to specifically speak about YouTube or Google, but normally when you use a system, for whatever application you use, they send you an improved version. Let's say it's version 6.1. They ask you if you consent, yes or no, and underneath the “yes” are the terms of acceptance, which are usually two pages of fine print that nobody reads. But if you actually push “yes”, by having done that, you have given explicit consent.

That's how all responsible applications work. This legislation basically forces everybody to do the same thing. Before I can put something on your system, I need your consent. It's up to you to read the consent or not.

Hon. Dan McTeague: Well, even on something that doesn't require my consent, say, my HTML, if I'm looking to use that as a means by which to access the Internet, which we all use, that too would probably be captured, potentially negatively, by this legislation. Take away the whole point of consent. I don't need consent nor does HTML send me a consent. I need it to function. It's the gasoline that makes the engine go.

Mr. Konrad W. von Finckenstein: Well, in that case, you give the consent. I mean, look at Adobe PDF. We all use it. That's how you read half your stuff. Adobe sends you a new version every six months or so. You consent to it. If you don't want to, you don't have to, but you do that it at your own peril, as it means you can't read new documents in the new format.

But it's your choice. All they are doing is giving you the choice. You decide what's more important to you: having access to the stuff from Adobe and Adobe offering you newer versions, or no, you want your privacy, and you pay the cost for it.

Hon. Dan McTeague: I just think that in the case of HTML it would be impossible to ask for consent. It's beyond.... I mean, I need it to access; it's part and parcel of what's there. Even before I can give consent, I need to have an HTML, so it's more than the chicken and the egg. But anyway, I'm hoping the commission may have given some thought to this in the process of deliberations.

Let me ask a final question, Chair, because it is one that I think goes to the core of what we're trying to achieve here.

There have been a number of summits in the past, with one in London and I think one in Asia-Pacific. To what extent is the CRTC involved with equivalent commissions beyond the United States? You talked specifically here about the Federal Trade Commission having the ability to work out a bilateral, but on a multilateral basis, what are the best fora and who shall speak for Canada in these kinds of organizations and these kinds of meetings? Is it one of the three departments or all three? Obviously, the Minister of Industry....

● (1820)

Mr. Konrad W. von Finckenstein: No. The overall policy for spam for electronic commerce, etc., clearly rests with the Department of Industry, and it's stated in the act.

Hon. Dan McTeague: I understand that.

Mr. Konrad W. von Finckenstein: It is the Department of Industry that usually goes to these fora. If an aspect is being discussed that is of particular relevance, let's say, to the CRTC, they might invite us to come and be part of their delegation, or we might ask to go with them, etc.

Hon. Dan McTeague: I'm just asking if it's you who would be discussing with the FTC that your recommendation should be adopted by this committee, or if it would be the Minister of Industry or the Minister of Trade.

Mr. Konrad W. von Finckenstein: If my amendment were adopted, I would be talking to the FTC and saying that we have the same provisions and asking them to please investigate.

Hon. Dan McTeague: Thank you, Mr. Chair.

The Chair: Thank you, Mr. McTeague.

Monsieur Bouchard.

[*Translation*]

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

Mr. von Finckenstein, you answered my questions and those of my colleagues very well. Earlier, we talked about the coordination between these three institutions. It is very clear that an individual who wishes to file a complaint must do so with one of the institutions. That is all very well.

What would you say if the bill provided for a one-stop shop for those citizens who wish to file a complaint? Do you feel that this would be a good provision?

Mr. Konrad W. von Finckenstein: When the government announced this bill, it said exactly what you have just said, namely, that there would be a one-stop shop for receiving complaints and forwarding them to the responsible organization.

As far as telephone complaints are concerned, we do have PhoneBusters. We could perhaps have some other organization, or PhoneBusters could be this one-stop shop for complaints. These complaints would be forwarded to us or to one of the other two responsible agencies. We would like to see this, but it is not part of the current bill. Perhaps the department will set up this one-stop shop.

The Chair: Thank you, Mr. Bouchard. Thank you, Mr. von Finckenstein.

Mr. Lake, it is your turn.

[*English*]

Mr. Lake.

Mr. Mike Lake: I have a quick follow-up comment after listening to Mr. McTeague's question.

I think there's a little bit of confusion between the two things we're talking about. On one hand, we're talking about the automatic update system that deals with the software programs we all have. We've talked about that quite a bit. It seems as if the legislation covers that adequately.

But I think Mr. McTeague is talking about things that just occur sort of naturally as you're surfing the Internet. There's a different kind of feedback, back and forth, that is automatic and crucial to the surfing experience in a sense.

The minister has said he's open to amendments. I think we recognize that there have to be amendments, minor tweaks in that area—and there will be.

That's just a point of clarification.

Hon. Dan McTeague: Mr. Chair, perhaps I'll just point out that I think it's a great argument for having me back on the committee. I'll do so only by unanimous consent.

The Chair: We welcome you any time, Mr. McTeague.

● (1825)

Hon. Dan McTeague: Thank you, Mr. Chair.

The Chair: Thank you to our witnesses for appearing today. Thank you to members of the committee.

I have one final point before we adjourn. For this committee's information, we were informed by the Privy Council Office that the Minister of Industry has appointed Lorne Brownsey to the board of directors of the Canadian Tourism Commission for a term of four years. This committee has 30 sitting days to review the appointment. If the committee wishes to review the appointment, we can do so in September.

Without further ado, this meeting is adjourned.

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

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

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

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

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