House of Commons
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 027 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, June 11, 2009

Chair

The Honourable Michael Chong

Standing Committee on Industry, Science and Technology

Thursday, June 11, 2009

● (1530)

[*English*]

The Chair (Hon. Michael Chong (Wellington—Halton Hills, CPC)): Good afternoon.

Welcome to the 27th meeting of the Standing Committee on Industry, Science and Technology. We are meeting pursuant to the order of reference of Friday, May 8, 2009, concerning Bill C-27, an act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act, and the Telecommunications Act.

We have in front of us today two organizations and three witnesses. We have Mr. Dennis Dayman, who is the secretary treasurer of the Coalition Against Unsolicited Commercial Email; we have Mr. Matthew Vernhout, also from the same organization, who acts as director at large; and finally, we have Mr. Michael Geist, who is appearing as an individual but who also serves as Canada research chair of Internet and e-commerce law at the University of Ottawa.

Welcome to all three of you.

We'll begin opening statements with Mr. Michael Geist.

Professor Michael Geist (Canada Research Chair, Internet and E-commerce Law, University of Ottawa, As an Individual): Thank you, Mr. Chair. Thanks for the invitation to come and speak.

My name, as you heard, is Michael Geist. I am a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I'm also a syndicated weekly columnist on law and technology issues for the*Toronto Star* and the *Ottawa Citizen*, and I was a member of the national task force on spam that was struck by the Minister of Industry at the time, in 2004. I served on the board of directors of the Canadian Internet Registration Authority, CIRA, for six years. I currently serve on the Privacy Commissioner of Canada's advisory committee. However, I appear today strictly in my personal capacity, representing my own views.

The introduction of Bill C-27 represents the culmination of years of effort to address concerns that Canada is rapidly emerging as a spam haven. I don't think I have to convince you that spam is a problem, whether it's the cost borne by consumers, schools, businesses, and hospitals in dealing with unwanted e-mail, or the shaken confidence of online banking customers who receive phished e-mail. There is a real need to address the problem.

I think we all know that Bill C-27 isn't going to eradicate the problem, but no country can do that alone. But I think it will finally help to clean up our backyard.

Members of this committee have noted that this is broad legislation that extends beyond just spam. I'd like to submit that this is a feature, not a bug. With much talk of the need for a national digital strategy, I think Bill C-27 fits nicely within that framework, providing much-needed consumer protection for electronic commerce. It's fair to say that the spam task force members recognize the need to address the broader issues towards the end of our mandate and that the steps in this bill are consistent with our recommendations.

While the legislation is broad, it's important to emphasize that the exceptions are broad as well. There are three exceptions, in particular, that I want to point to.

The first exception is consent. Under this law consent trumps all. Indeed, any business or any organization can do anything it likes with respect to electronic marketing or software installation as long as it obtains consent. Now, there are some rules around that consent—form requirements for electronic marketing, disclosure requirements for the software—but I don't think it's an onerous obligation. In fact, whenever a potential concern is raised, and I know that some have been, the first question to ask is, “Why is obtaining consent unreasonable in those circumstances?” Is it unreasonable to ask someone to obtain consent before installing a software program on my computer? Or is it unreasonable to obtain consent before sending me a commercial e-mail about a house sale or about a product or a service? I think in almost every instance the answer is no, that consent is a reasonable requirement.

Moreover, it's not an uncommon requirement, as other laws have adopted the same opt-in consent model. Australia and New Zealand both have opt-in models, and Japan actually switched from an opt-out model to an opt-in model when they found that their opt-out model didn't work.

Secondly, there is a business-to-business exception, as you know. I've heard some claims that this legislation will hamper business as it seeks to use e-mail to promote its products and services to other businesses. The reality is that the legislation contains a business-to-business exception, paragraph 6.(5)(b). I think many of those concerns are unwarranted.

And finally, there are the consumer exceptions. These are pretty broad—in fact, arguably too broad. They mirror, for the most part, the exceptions that we find in the national do-not-call list. I think there are many people who argue that those exceptions already go too far.

Consider, for example, the business-to-consumer exception that covers eighteen months for existing customers and six months for non-customers who merely make an inquiry. So think about what that means. Somebody makes an inquiry with a long-distance provider about one of their plans or contacts a hotel to see if they have room availability and they are then subjected to six months of electronic messages under the guise that this is now implied consent. I think it's reasonable to ask why a business should be entitled to contact a consumer for six months without any further consent merely because the consumer has made a single inquiry.

My point here is that the net of the legislation may be broad, but so too are the exceptions that will continue to permit commercial activity. Some businesses may argue that it goes too far, and some consumers may believe it doesn't go far enough. Perhaps that's a sign that an appropriate balance has been struck.

Let me quickly talk about how these principles apply to several of the criticisms that I saw highlighted earlier this week. I know jurisdiction was raised. And jurisdiction, as you know, covers connections with Canada, including the routing of a message through Canada. This approach merely builds on existing jurisdictional law in Canada with respect to a real and substantial connection. If a message fleetingly enters Canada, I suspect that the test would not be met of a real and substantial connection and it's a non-issue from a liability perspective.

With respect to software updates, as I referenced earlier, it seems perfectly reasonable to expect a software vendor to obtain consent from an end user before installing anything on their personal computer and to tell them what they are about to install. To suggest otherwise would be to surrender control over their personal computer and to face the prospect of security breaches, as occurred in the fairly infamous Sony rootkit case.

● (1535)

Then there's the issue of real estate agent e-mails. As I'm sure many of you are aware, real estate scams are among the most common, with references to swampland in Florida being almost shorthand for the notion of fraudulent offers. Do we really want to exempt an entire area that suffers significantly from spam concerns?

Fourth, there's the issue of tough penalties, including the private right of action. I'd argue this is another feature of the legislation. The bill has tough penalties. The experience in countries such as Australia has been that anti-spam law only works if the penalties are sufficiently tough that you create some economic risk for spammers. Otherwise, they simply keep on doing what they're doing. In fact, there have been some lawsuits launched against Canadian spammers, but they've been launched elsewhere because Canadian law didn't measure up. I think we ought to fix that.

Are there any changes needed? I think there are at least two amendments I can point to. The first—and it was raised by this committee—is the prospect of a review provision. I think it's a fast-moving area, and mandated reviews make sense. The second involves the computer software consent provision. In the main, I think the provision gets it right. However, there may be a limited number of instances—the use of Java script on web pages comes to mind—where the provision could prove problematic. It's not easy to craft a rule that targets all the harms, the botnets, spyware, surreptitious installations, keystroke logging, while leaving behind the benign activities.

I'd suggest a small addition. I'm not a legislative drafter, but I would suggest essentially a subclause 10(3) that would allow for implied consent for certain types of computer programs where the person has consented to the installation of that type of program by way of their preferences in their web browser. In other words, if they've checked their preferences in their browser that will allow that form of program, then we ought to be able to take that as implied consent. That would cover off programs like Java and Java script, as those are typically addressed within web browser preferences.

Let me conclude with a warning against what I see as some lobbying efforts to water down what I see as reasonable standards found in this legislation. I'd note that we have seen this before; it's what took place with the do-not-call list. That bill started with good principles, faced intense lobbying and I think some scare tactics, and by the end of the process Canadians were left with a system that I think is now widely recognized as a failure, with some estimates saying that more than 80% of the calls that used to come continue to come, and with security breaches around the do-not-call list itself.

I think we must avoid a similar occurrence with respect to anti-spam legislation. Change in some business practices might be scary to some, but we can't allow scare tactics to dissuade you from moving forward with this much-needed legislation.

I look forward to your questions.

The Chair: Thank you, Dr. Geist.

Mr. Dayman.

Mr. Dennis Dayman (Secretary Treasurer, CAUCE North America, Inc.): Thank you.

Good afternoon, ladies and gentlemen.

[*Translation*]

My name is Dennis Dayman.

[*English*]

I'm the secretary treasurer of the Coalition Against Unsolicited Commercial E-Mail, or CAUCE. With me today is Matthew Vernhout, one of CAUCE's directors at- arge, who's on the anti-spam task force as well.

CAUCE is a group representing computer users in Canada and the rest of North America. CAUCE thanks you for the opportunity to speak to Bill C-27, the Electronic Commerce Protection Act.

As you can probably tell by my accent,

● (1540)

[*Translation*]

I am not Canadian; I am American.

[*English*]

And I regret that I do not speak French.

So why is an American here today addressing this esteemed committee? Well, reflecting the way in which spam is a global problem, some years ago CAUCE Canada merged with its American counterparts to better serve our constituents. Spam respects no borders, and to best represent computer users on both sides of our mutual border, we decided to mount a coherent Can-Am front against the blight of Spam 2.0.

Spam 2.0 might be a new phrase to you. At the turn of the millennium, virus-makers, hackers, spyware producers, phishers, and spammers joined forces in a blended threat, and spam is a distribution mechanism for their evil. It's now not merely a conveyance of illicit marketing, but also of malware of all shapes and sizes. Phishing, spyware, viruses, and spam are all now the products of the same criminals. Spam isn't just in e-mail any more. It comes to us by text messaging, voice over IP, our social networking sites, and instant messaging.

Bill C-27 recognizes this, and we in the consumer advocacy and marketing community thank the drafters of this bill for having taken a smart, open-minded, broad approach to current and future threats.

You heard me correctly, ladies and gentlemen. CAUCE, once the exclusive domain of the computer geek anti-spammers, has openly embraced the marketing community for a decade now. It counts among its members and executives many individuals and companies who have an enlightened view as to why anti-spam laws work in our favour.

My colleague Matthew Vernhout and I work for large international e-mail service providers. I work for Eloqua Corporation, and Matthew is at ThinData, Canada's largest e-mail service provider. Both of our companies were founded and continue to operate in Toronto. Our companies provide sending infrastructure for marketing e-mail on behalf of such companies as Fidelity, Air Canada, American Express, and literally hundreds of small and medium-sized companies. We are very much in favour of this law.

By now, you have received many letters supporting Bill C-27 from others in our community, such as Matthew Blumberg, the CEO of Return Path Inc. Return Path certifies commercial marketing e-mail into such places as Hotmail, Yahoo!, Telus, Bell Canada's Sympatico, and literally hundreds of other large and medium-sized Internet service providers.

It is our understanding that some have been spreading what we in the Internet community call FUD—fear, uncertainty, and doubt—about this bill. We cannot understand why anyone is doing so. Perhaps it's an adversarial relationship with some of the enforcement agencies in this country. Perhaps it is to create a hostile business environment for competitors. Some, perhaps, benefit financially from providing connectivity to those bad actors.

What we do know is that this bill has a long tail. It directly intersects with American and Canadian marketers and consumers. And we are here to assure you that from the standpoint of legitimate international and Canadian-based marketing companies, the bill is well crafted. We have no worries about our clients' e-mail or our professional activities.

Bill C-27 has broadband support on both sides of the equation—sending ESPs and receiving ISPs.

Bill C-27 draws from the experience and builds on the success of laws elsewhere, cherry-picking the best aspects of laws in, for instance, New Zealand, America, and Australia. Australia, for example, has had great success with the private right of action aspect of the law. Legitimate businesses continue apace, while bad senders have suffered the consequences, much to the benefit of good players.

Some might tell you that the law is complicated. CAUCE does not disagree. Yet the portions dealing with the problem of spam are simple and direct. They are already industry best practices, and many have already been implemented. Necessarily complicated are those aspects specifying the new Canadian enforcement regime. It would be folly for the one G-8 country without anti-spam legislation, Canada, to wait for agency reform prior to passing what is long overdue. Hence, we concur with this bill's approach of giving increased powers to existing enforcement agencies.

Canada must do its part to deal with homegrown spammers. Despite what you might have heard, Canada, with solid and inexpensive broadband infrastructure, is home to some of the most expansive spamming networks.

Canada has the highest per capita membership on the social network site Facebook, which is why a Lachine, Quebec, resident took advantage of their systems. He was successfully sued under the American CAN-SPAM law for three-quarters of a billion dollars. The spammer is now claiming to have zero assets, yet his blog indicates that he dines at some of Montreal's finest restaurants. Clearly, he has some pocket money. It is our understanding that Facebook is very actively investigating options in terms of getting a judgment here to seize what he does have.

Another example of Canadian spam is a man who lives near Montreal. His company has spammed for ten years, unabated, to promote the Canadian government subsidy directory. Despite repeated complaints to the Office of the Privacy Commissioner, the spam continues to this day, hitting the inboxes of virtually all CAUCE directors, and I imagine yours as well.

● (1545)

And let us not forget our west coast. There is a company whose scheme is more complicated. It produces herbal concoctions designed to attempt to get around the health laws of the country. Their snake oil promises to help you stop smoking, lose weight, or, alternatively, grow larger in certain areas. They have been successfully sued in the United States under a class action lawsuit because, not surprisingly, this stuff does not work. The company is owned by two brothers. Their substances are produced in the Caribbean and shipped to a British Columbia distribution centre, and their marketing e-mail originates from there as well. They don't spam on their own behalf, apparently. Rather, they have what they call "affiliate programs" where people, real or imagined, sign up to earn a commission and send promotional e-mails—spam—to drive those sales. The spam is sent from all over the world. The company maintains a veneer of false legitimacy and clean hands.

Thankfully, here too Bill C-27 does bring a remedy. The beneficiary who profits from illicit activities is on the hook. Such a company would be shut down were this bill to become law. The infamous Canadian pharmacy spam gang got its start in Montreal and has points of presence in eastern Europe, with major ties to organized crime.

For these reasons, ladies and gentlemen, CAUCE speaks for tens of thousands of Internet end users and legitimate companies with a horse in this race when we respectfully encourage you to pass this law as quickly as possible to help clean up the Internet for the benefit of all. Canada must do its part, and Bill C-27 is a significant solution to that spam problem.

Thank you, and we will be happy to take any questions you may have at this time. Merci.

The Chair: Thank you, Mr. Dayman.

We'll have about an hour and a quarter of questions and comments from members of this committee.

We use both official languages here, so if you need translation there are earpieces provided.

We'll begin with Madam Coady.

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

Thank you for appearing before us today. We appreciate your taking the time to join us and bring your expertise and enthusiasm for this bill. I'm sure I speak for all my colleagues around this table: everyone is anti-spam, if I can use that term. We just want to make sure we have the best legislation possible, so thank you for taking the time today to share with us your stories and expertise.

I only have about seven minutes, so I'm going to be kind of rapid-fire in some of my questions. I'd appreciate it if I could get very rapid-fire responses.

First of all, Bill C-27 is very broad in scope in some of its definitions and very narrow in some of its exceptions. Mr. Geist, you pointed that out right from the very beginning of your testimony, talking about how the broad scope kind of captures all of what we're trying to deal with here in terms of anti-spam, but the exceptions really are defined. I think your view is that the bill itself does a good job in giving some of those exceptions. Did I capture that kind of neatly?

Prof. Michael Geist: I wouldn't have described the exceptions as narrow, actually, but quite the opposite. I believe the exceptions are very broad, and that's perhaps an attempt to strike the right balance.

Ms. Siobhan Coady: Let's come to that; that's where I'm leading. My view on this legislation is that it basically captures all commercial messages, and then the exceptions kind of pop out anything that shouldn't be there. When I look at some of our international colleagues, the CAN-SPAM, Australia—I think you've used it as an example—Singapore, U.K., New Zealand, they more define it towards direct marketing. They use direct marketing versus that kind of broad consent. I'd like your view on that, but I'm going to come to that, and I've got some more questions, so I want you to just keep that in mind—ours is kind of broad, to keep everything, all commercial electronic messages, versus our international colleagues using direct marketing. I'll use that term to more narrowly define it.

On consent, I'm concerned about some of the narrow provisions, the narrow definitions. So the first question is to compare and contrast our international colleagues who look at direct marketing versus the broad definition we're using. And concerning consent, I think we are narrowly defining it—and you can express your opinion around this—because ours talks about consent being expressed or implied. However, our consent is implied only where the person who sends the message has an existing narrowly defined business or non-business relationship with the person who receives the e-mail. I'll give you some examples of that, but I'll pause for a moment to get your reaction to that.

● (1550)

Prof. Michael Geist: Sure.

With respect to Australia, respectfully, my reading is different. I have the Australian act in front of me, and it refers to commercial electronic messages in much the same way. I don't see a significant difference on the definitional side.

Part 2, subsection 16(1), of the Australian act says:

> A person must not send, or cause to be sent, a commercial electronic message that...has an Australian link...and...is not a designated commercial electronic message.

Then you go into the definitions.

It frankly mirrors a lot of what we've done. I think it was noted by my colleague here that it's pretty clear Canada borrowed fairly heavily from the legislation you find in other countries. So I actually don't see the first premise; I don't see that focus on direct marketing the way that you suggested. I see statutes that talk about commercial electronic messages in much the same way we do.

Then you get into this other basket. As I mentioned off the top, everything is permitted; there's nothing that you can't do. The only question is whether or not you have to get someone's consent in order to do it. The exceptions we're talking about—the notion of a business, for 18 months after they have an actual relationship, or six months after an enquiry, or political parties, or charities, and all these other exceptions—are exceptions to the notion that they don't even need to get that.

That strikes me as providing pretty wide latitude. All a business has to do in every one of these circumstances is get consent from the customer; then they're okay.

Then you get into the second basket, where you say "I don't want to get consent from the customer", and we're still giving them quite a wide berth to continue to market to consumers.

Ms. Siobhan Coady: Can you talk about educational facilities and organizations for a moment?

Prof. Michael Geist: I know that under "do not call", educational institutions have fallen under charitable organizations, so they might well fall under the same here.

Ms. Siobhan Coady: The Australian Spam Act that you referred to gives exceptions. It excludes designated commercial electronic messages that contain factual information from, for example, government bodies, educational institutions, religious organizations, etc.

Prof. Michael Geist: That's right, but our bill—I'll try to find the specific section—contains an exception for, I believe, registered charities. To my knowledge, just about every single university, for example, that might want to contact an alumnus is a registered charity. I know that's the approach under "do not call" that's being taken by all of those organizations.

Ms. Siobhan Coady: Your understanding is that this would fall under that premise, and you wouldn't have any concerns about it?

Prof. Michael Geist: That's right.

Ms. Siobhan Coady: Okay.

Would you care to comment, Mr. Vernhout? I don't mean to cut you out of the conversation. Is there any comment?

Mr. Matthew Vernhout (Director-at-large, CAUCE North America, Inc.): I think that direct marketing is a part of that, maybe a subset of electronic commerce, direct marketing being more by way of an e-mailed, targeted conversation with an individual and electronic commerce looking more into social networking, IM, and voice over IP. It's a portion of, rather than the whole.

Ms. Siobhan Coady: Here is one final, quick question. I'm bouncing all over the place here. This is the private right to action. You're familiar with the private right to action.

I'm going to look at the state of Utah. You may be familiar with this in the case law. They had under their statute that particular provision—it was a little different, but it was that particular provision—yet it was repealed. Would you care to comment?

Prof. Michael Geist: My understanding is that in Utah you had widespread abuse or attempted abuse of that provision. I think it was prisoners who were sending messages and then hoping to use that as an opportunity to file suit.

While I recognize that this seems like a concern, the experience we've seen in Canada is that our litigation environment is quite different from that in the United States. Things such as costs are different. Filing frivolous suits under a private right of action could well leave someone facing some of their own court costs, if they were to do that. We already have some disincentives built into the process.

When we look at the overall picture and at the number of large players who have wanted to target some of the Canadian-based spammers we have heard about, we see that they have been clearly unable to do so in Canada. Indeed, in the Facebook example—and we have seen it in other cases too—they have had to sue under U.S. law against Canadian-based spammers, because of the absence of legislation to deal with it here.

● (1555)

The Chair: Thank you very much, Dr. Geist.

[*Translation*]

Mr. Bouchard, you have the floor.

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

I wish to thank you for being here with us this afternoon and for your participation.

My first question is for Mr. Geist, Canada Research Chair in Internet and E-Commerce Law.

Mr. Geist, unless I am mistaken, you are opposed to Bill C-27, because you do not consider it to be strict enough. Is that correct? Please correct me if I am mistaken.

[*English*]

Prof. Michael Geist: No, and I'm sorry if I wasn't sufficiently clear. I'm supportive of Bill C-27. My concern lies with the potential to water down the legislation. I think it does a pretty good job of striking the balance, and my fear is that some of the concerns, many of which I think are not valid once you take a look at the legislation, will result in a weakening of the legislation itself.

So I'm supportive, and supportive in much the form in which we see it now.

[*Translation*]

Mr. Robert Bouchard: In Bill C-27, mention is made of international cooperation. Given that a lot of spam originates from elsewhere, Bill C-27 asks that we cooperate with other countries. No powers are therefore being granted to the enforcement agency responsible for this bill.

Should we be forcing the agency responsible for enforcing Bill C-27 to negotiate agreements with other countries in order to reduce spam?

[*English*]

Prof. Michael Geist: It's a great question. I think in some ways there are already frameworks in place to deal with many of these international issues. Canada has been a participant in them. Even dating back to when we were sitting as a spam task force, groups called the London Action Plan were bringing together various countries in an effort to deal with it. In fact, in many ways, that really highlighted how Canada was trailing behind many of our trading partners in our peer countries in not moving forward with legislation.

In some ways, we already have some of that framework in place, whether it's through the OECD or the London Action Plan or some of the groups these gentlemen are involved with. There are already those linkages. What has been missing is the legislative piece. One would hope that some of the people who through Industry Canada and otherwise have been actively involved would continue to be involved, because we already have many of those linkages with similarly placed authorities in other countries.

[*Translation*]

Mr. Robert Bouchard: I was surprised to hear you say that the Do Not Call list was a failure. When he appeared at the last Committee meeting, the minister told us about the great success of the list.

I know nothing at all about the matter, but in what is the list a failure in your eyes?

[*English*]

Prof. Michael Geist: My sense was that the minister recognized it was still early days and that there perhaps have been some growing pains with respect to the do-not-call list. I think it's more serious than that. There are more than six million numbers registered on the do-not-call list. There have been well-publicized incidents in which those numbers have been put out in the clear, and people have been misusing those numbers.

There are so many exceptions within this legislation. And note that when the do-not-call legislation was introduced, there were no exceptions. After much of the lobbying and scare tactics about what this would mean for business, we ended up with so many exceptions that now, as I say, estimates are that at least 80% of the calls that were permitted before are still permitted today.

We have also had huge enforcement problems. According to the CRTC, they have not yet lodged any formal complaints, other than warning letters, under any of the complaints that have been filed against spammers, despite the fact that we have seen thousands of complaints under the do-not-call list. By my definition, that, at least to date, counts as a failure.

[*Translation*]

Mr. Robert Bouchard: Thank you very much.

I now have a question for the other group.

You struck me as being much more positive. You are in favour of the bill, and I even took your statements as meaning that you consider it to be perfect.

With regard to foreign spam, would you have recommendations or advice to give us in order that we be more effective? You are aware that the aim of Bill C-27 is to reduce or eliminate spam here in Canada.

I would like to hear what you have to say about some mechanism or improvements that might be made to Bill C-27 with regard to spam originating from outside Canada.

● (1600)

[*English*]

Mr. Dennis Dayman: It's my understanding that Bill C-27 follows the money. Most domestic spammers or Canadian spammers today tend to e-mail offshore, to get around blocking techniques and other laws that might be out there. But in general, the way I interpret the law—and Matthew might want to also make a comment on this—it follows the money. So even if we have spammers who are Canadian-based, who are attempting to get away from the law, trying to get away from blocking techniques, the bill itself will follow up with them through the illicit profits they would make.

Matthew?

Mr. Matthew Vernhout: I would agree that the way we've understood it and the way we've interpreted it is that the party being advertised is equally responsible for the sending of the message and therefore under the law would be considered responsible and therefore actionable.

[*Translation*]

The Chair: Do you have another question?

Mr. Robert Bouchard: No, not for now.

The Chair: Thank you, Mr. Bouchard.

Mr. Lake.

[*English*]

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

My first question is for Mr. Geist. I know you were present at the first committee meeting we had on this, so you heard this. There were a couple of concerns brought up by members of the committee, and I'll quote them:

> The net being cast so broadly has also left certain definitions so general that the interpretation of something as simple as a computer program can be taken in a number of ways.

That was one quote. Another member said:

> That is my concern with this legislation. It's the fact that it has a very wide net that impedes business from taking place.

We're in a world where we have technology changing very rapidly, and I would think it would be a concern when you're putting forward this kind of legislation that technology could change so rapidly, you'd have to be introducing new legislation every year if you don't have that wider net.

Maybe you could comment on the need to have that little bit wider net when you're dealing with this particular type of legislation.

Prof. Michael Geist: Sure, and I think that's absolutely right. Quite frankly, we experienced the concern as a task force ourselves. It was a year-long process. When we started the focus was almost exclusively on spam, and by the end of the 12 months, issues around spyware and phishing had really emerged as key concerns. Even just within that 12 months we saw just how rapidly this was moving, and of course that has continued to happen over time.

If you take a look at what the successful forms of legislation are with respect to anti-spam legislation, they necessarily try to be as neutral as possible in terms of casting somewhat of a wide net. The way you counter that, to preserve the concerns of business, is to create sufficiently broad exceptions. As I've tried to argue, if anything, these exceptions may be overly broad on the business side. When a business can simply ask for consent and is still accepted in a whole slew of other areas, I don't think there ought to be any kind of concern that legitimate business is going to be significantly impeded.

Mr. Mike Lake: All right.

I want to deal with the issues of concerns that folks have brought up, and perhaps you can respond to them. I note in an article from *Network World Canada*, there is a quote here from discussions around concerns that a Canadian lawyer has regarding the legislation. In the article, the lawyer from the Canadian law firm suggests:

> To comply with the law, companies would have to overhaul their Web sites to force users to click on a button agreeing to every download, signifying their expressed consent.

Then the quote from the individual:

> It's just overkill. The bill as currently drafted would actually ban the use of the Internet by Canadians unless a person with a Web site had written consent from a consumer to use it.

Then the quote from the article finishes by saying:

> Instead of demanding consent for certain activities, Ottawa should define activity that's bad—for example, creating misleading e-mail headers.

What are your comments on that concern?

Prof. Michael Geist: I think I'm quoted in that same piece.

Another one of the concerns was that someone might want to buy software from a software vendor, and if it was outside of the 18 months, the person they're buying from might report the consumer as a spammer, which I didn't think was a particularly significant concern.

I frankly don't think many of those other concerns are realistic either. The truth of the matter is, if the concern is around the definition of a computer program—and I alluded to that in my opening—I think we have the ability to address the very narrow concerns that may be raised by that broad definition. So there's the issue, for example, of Java script, where if someone is accessing a web page, it runs automatically. In that sense, yes, you'd need to obtain consent. If we can exclude that kind of automated program where someone has effectively already provided consent by virtue of their preferences on their web browser, I think we actually deal with that.

For other instances, when we are talking about software programs that are downloaded, then absolutely you ought to obtain consent. The whole premise of spyware is that this stuff is inserted surreptitiously into people's computers without their notice or consent. The whole problem with the Sony rootkit case was when someone went to put a music CD into their program, it installed things on their computer without their knowledge and engaged in surreptitious activity. That's precisely what we're trying to stop, and the legislation tries to do exactly that.

● (1605)

Mr. Mike Lake: You mentioned legislation in other countries. Obviously you've done some significant study of such legislation. In terms of your study, what can you tell us about two things: problems in the legislation of other countries that these countries have addressed proactively, that is, they've recognized the problems and have addressed them; and maybe problems in the legislation of other countries that should be addressed, but maybe haven't been addressed yet, but that commentators have noted, and you agree, should be addressed?

Prof. Michael Geist: With respect to problems, here are two that I think highlight why in fact Bill C-27 does a pretty good job of dealing with these issues. The first problem is on this issue of whether it's opt-in or opt-out. I'm a strong supporter of our move towards an opt-in model here. As I think the minister noted, it could potentially serve as the model for the do-not-call list down the road. That's obviously embedded in this legislation as well.

If you take a look at what the Japanese did, they started with an opt-out. They started by saying you get a kick at the can and can send all the e-mails you like, and if someone says they don't want to receive your e-mail any more, you have to take them off the list. They quickly found that does not work. The better or friendlier approach from a consumer perspective, from a privacy perspective, and frankly from a good business perspective and confidence perspective is an opt-in model. They switched to the opt-in model.

The other country I'd point to is actually the United States. In this instance, they were one of the first off the mark with their CAN-SPAM Act. They were very narrow in it; they dealt just with spam. A lot of people feel they didn't deal with it that well, even within CAN-SPAM. But what we have seen in the U.S. since CAN-SPAM are successive state laws that try to deal with spam, and federal laws that try to deal with spyware, specifically because they didn't cast the net broadly enough. So they have continually tried to play catch-up with new legislation, either at the federal level or state level.

The way to deal with this is actually to learn from those lessons, and I think that's what Bill C-27 tries to do.

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

Madam Crowder.

Ms. Jean Crowder (Nanaimo—Cowichan, NDP): Thank you, Mr. Chair.

I want to thank the witnesses for coming before the committee.

This first question is for Dr. Geist. It's probably not surprising that I want to talk about the do-not-call list. In an article of April 28, you indicated that "The complicating factor is that the ECPA provisions related to the do-not-call list are exceptionally complicated and could be delayed for years."

I just want to touch for a minute on the legislative summary. Maybe you can help us make some sense of this. It says:

> Clause 6(7) is noteworthy, since it exempts two-way voice communication between individuals..., which would normally mean that telemarketing activities covered by the DNCL are exempted from the ECPA. However, later in the ECPA, clause 64 provides for the repeal of this exemption provision, which appears to indicate that while telemarketing activities covered by the DNCL may be exempt from the ECPA in the early stages of the Act's implementation, it may be speculated that the government intends to eliminate that exemption at a later date. This would mean that all the requirements included in clause 6 of the ECPA would eventually become applicable to telemarketing activities as well, including a much more stringent consent standard than currently applied under the DNCL.

Is that an accurate reflection of where you think this piece of legislation is going?

Prof. Michael Geist: I will admit, it's something I haven't much seen in legislation. I found it was a surprising inclusion in this bill, having worked through 68 pages, to find at the very end provisions that would effectively kill the do-not-call list and replace it with this legislation.

My own view, given the challenges and problems we've seen with the do-not-call list, is that this would actually be a better approach. Rather than facing the kinds of security issues we've seen around the do-not-call list, this would eliminate that by setting a stronger standard, so we don't have lists of six million numbers literally being floated around the world, with people getting all of these calls they don't want.

So the theory behind this is good. Now, the practice of it is rather awkward, because it says, on the one hand, that it's excluded, and then, as I think this committee heard on Tuesday, this is basically creating the prospect at some point in time in the future of pulling the plug on the DNCL and having this in its place. It's nice to know that it's in its place. If it were up to me, I would say pull the plug now and have this apply universally to both electronic communications and telemarketing.

● (1610)

Ms. Jean Crowder: It seems a somewhat odd approach that embedded in a piece of legislation is this clause saying that sometime in the future, the government may.... It's surprising to me they didn't deal with it in this context, where they've already written the language that would address it.

Prof. Michael Geist: I'm loath to read into what exactly the full thought process was in terms of making that choice, although I might guess that it is, admittedly, early days. The do-not-call list has only been up for a year, although I think there's enough evidence to suggest that changes are needed.

Perhaps given both the time and investment that's gone into this, some would be of the view that it is premature to take that step to say we're going to change course just months after we started with, at long last, this do-not-call list. So I can understand that thinking, although at the same time—and I thought the minister actually acknowledged this—the reality is that we're making distinctions where they increasingly don't exist. The notion that it's telemarketing or it's text-messaged spam or it's e-mail spam I think for many people is all part of the same basket.

I think this is foreshadowing making, at the end of the day, a choice, and the choice is the opt-in approach that we've seen within ECPA. I think we do better by making that choice right now, though, and just saying, "We've seen what has happened with the do-not-call list. There are too many Canadians right now who are getting unwanted calls. Let's switch to something we think is going to be more effective and is going to deal with both telemarketing and electronic communications."

Ms. Jean Crowder: Am I to presume, then, that some of the difficulties you identified with the do-not-call list in that same article, in terms of the investigation of complaints and what not for the do-not-call list, have not been addressed, then?

Prof. Michael Geist: There's no attempt to fix anything within the do-not-call list in this legislation. It's merely to say that at some point in time we almost have this poison pill where we can stop the do-not-call list and replace it with the ECPA.

I would say that if the decision to stick with that approach, that almost two-track approach, is maintained, it's incumbent to address the problems that we right now have within the do-not-call list. I think it's astonishing to think that we have had what must rank as one of the largest security breaches in this country's history, when you think about six million Canadian phone numbers just out there, with people getting all sorts of phone calls, unwanted now, that they never used to get, and nothing has happened. It's astonishing when we look at the thousands of complaints that are being launched and we have had no investigations beyond complaint letters by the CRTC, when we look, frankly, at the exceptions....

I launched an access-to-information request where I literally got thousands of pages of the complaints that have been filed about the do-not-call list. I'll tell you that it's a lot of the big everyday companies. Canadians have registered their numbers and don't think they're going to get calls any more, and they continue to get calls, many of which are now still permitted under this legislation. I'm deeply worried that we're going to replicate that kind of approach in this law, where Canadians are going to have the expectation that at least legitimate marketers in Canada are going to stop, and yet there are going to be new loopholes here that are going to allow them to continue.

Ms. Jean Crowder: I guess, for me, having something put in a piece of legislation that is absolutely—and this isn't a partisan remark—at the government's discretion is troubling. It seems far better to have dealt with it upfront.

In your presentation you talked about mandating a review process, and I want to turn to the *Stopping Spam* task force report. In recommendation 22 it reads: "The federal government, through this coordinating body, should monitor the impact of the implementation...", and so on. It had a number of things: monitoring the impact, evaluating the results, providing regular public reports, consulting with stakeholders. Is that the kind of process you're recommending in terms of a mandated review?

Prof. Michael Geist: No, I was thinking of a legislative review. I do think that is obviously necessary. Reporting requirements to get a sense of how effective this legislation is on a regular basis and what we're doing internationally are the sorts of things I think we ought to be doing, and they surely ought to be baked into the rollout. At the same time, my experience in some of the other areas is that by including some sort of mandated review, it provides that opportunity to ensure that we get it right.

If new issues have emerged that the net perhaps wasn't cast as widely as it should have been, it creates that opportunity to try to address those issues, whereas if there isn't that mandated review directly in the legislation it sometimes can be hard to get the necessary attention.

● (1615)

The Chair: Thank you, Madam Crowder.

Thank you, Dr. Geist.

Mr. Garneau.

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

Thank you very much, all of you, for coming today. I want to assure you that I am also very eager to combat spam. I just want to mention that from the outset. I also want to make sure that it's the best possible bill, so that we're not squashing a fly with a sledgehammer. It's not an easy thing to avoid.

I have some questions.

Concerning address harvesting, the provisions that are in here, some interpretations of the address-harvesting prohibitions would make it illegal for law and order authorities to collect information in the case of suspects involved in bank fraud, ID theft, online extortion, possibly online harassment, possibly child pornography, and other issues. What is your interpretation of the way the address-harvesting provisions are written in this bill at the moment?

Prof. Michael Geist: I must say that's the first time I've heard that particular complaint. I believe there is an exception for law enforcement. If there isn't an exception for law enforcement dealing with that, then there ought to be.

Mr. Marc Garneau: Do you have anything to add?

Mr. Dennis Dayman: That was my understanding as well, sir, that there's an exception in there. I'd have to go back and check, unfortunately.

Mr. Matthew Vernhout: I think the idea behind address harvesting, as well, is more for the purpose of building a list to send e-mail to. It's a case of going to websites and looking for people who have published addresses and then subscribing them to a list and, in theory, just spamming to them.

Mr. Marc Garneau: Exactly. That would definitely be the purpose, yes.

Let me ask you about some examples of what might be considered spam under the bill as currently written.

A business that sends an electronic message that provides warranty, product recall, safety or security information about goods purchased more than 18 months previously, is that an example of spam, in your opinion?

Prof. Michael Geist: It's not, and it's not a problem under this bill. If I purchase a car seat for my daughter and send in the warranty card and give them consent to send me regular updates, as I no doubt would, because I'm going to be concerned about the prospect of safety recalls, then they can continue—and I would hope that they would—to send me any of that information. All they have to do is to obtain the necessary consent. It's open to the consumer in every instance to ensure they get that warranty information.

Mr. Marc Garneau: So you're saying that if the consent has not been given, it would constitute spam.

Prof. Michael Geist: I'm saying that if it is outside the 18 months and the consumer didn't give consent for that warranty information to be sent to them, then I suppose, yes, it might be.

Mr. Marc Garneau: If that process of filling out forms, or whatever, at the front end was not undertaken, then it would constitute spam.

Prof. Michael Geist: Well, if they didn't fill it out, I'm not sure how the business would contact the individual.

Mr. Marc Garneau: Perhaps they sold them a car, or something.

Prof. Michael Geist: Right. At the time the person has made that purchase.... We all fill out these cards all the time for production information and the like. But all they have to do, any time they're obtaining that information in the first place, is to obtain consent. If they've never obtained my personal information, then they're not going to be able to send me any of that product or warranty information in the first place. So all we're doing is asking a business at the time they collect that information in the first place to get the consent.

Mr. Marc Garneau: So what we're saying is that the business must now make sure they get that consent at the front-end.

For a business that sends out an electronic message that provides information about product updates or upgrades that a person is entitled to receive for a product purchased more than 18 months previously, I guess you would say the same applies.

What about sending newsletters, business publications, or company information from anyone who has made an inquiry about a company's products or services more than six months before?

Prof. Michael Geist: If we're talking about business-to-business, it's excluded.

Mr. Marc Garneau: I'm not talking about business-to-business.

Prof. Michael Geist: If you're talking about business-to-consumer, then, yes, exclude it.

Mr. Marc Garneau: What about sending university alumni information in a newsletter, if that alumni letter has some advertising in it?

Prof. Michael Geist: As I mentioned to one of your colleagues, there is an exception for charities. So if you're registered, I think it's section—

Mr. Marc Garneau: No, I'm talking about an advertisement for you to buy something, but it's in the newsletter.

Prof. Michael Geist: Right. I think if the gist of the overall message is that it's coming from a university, let's say, which is a registered charity, and within it there's an opportunity to get a university-branded credit card, or something like that—which we often see—I think it would still be permitted within this particular exception.

Mr. Marc Garneau: What if it's not that kind of an ad, but something more commercial?

● (1620)

Prof. Michael Geist: If it's strictly a commercial message and it falls outside of this exception, so we're dealing with something that's clearly commercial, then you have to obtain consent.

Mr. Marc Garneau: Something I've asked a number of people about, but haven't had a clear answer on, is the issue of cookies. How do you view cookies? Are they spam, in your opinion, or not?

Mr. Dennis Dayman: Our company, Eloqua, is a company that helps other companies generate lists and prospects. We do that by enticing or giving technology to our customers to entice other people to come and register and actually take an action—to put in their name, e-mail address, and a phone number. They basically opt into a newsletter, and sometimes even opt into being tracked. What we try to do from a product standpoint is to tell companies who is visiting their website, and who is interested in what's going on. In most ways, I don't really consider cookies spam, especially from the standpoint that we are very clear about what the information is going to be used for, especially in our privacy policy at our company Eloqua, or even within our own customers' privacy policies. So I do not consider cookies spam.

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

Mr. Geist, go ahead.

Prof. Michael Geist: I'll take 15 seconds just to supplement that. The issue of cookies has come up in discussion, not so much as to whether it's spam but as to whether it's a computer program that's being inserted on someone's personal computer. I think the consensus is that it is not.

If you take a look at standard definitions for what a cookie is, it is simply a text file that is inserted onto a personal computer, at the user's request; they have the ability not to have it there. It doesn't run anything, and if you take a look at the definition of software programs referred to here, they require something more than just being a text file itself.

The Chair: Mr. Garneau.

Mr. Marc Garneau: Does the computer program definition in this legislation exclude the text file?

Prof. Michael Geist: Yes, I think it does.

The Chair: Thank you very much, Dr. Geist and Mr. Garneau.

We'll continue our discussion of cookies and SMTP, otherwise known as e-mail.

Mr. Warkentin.

Mr. Chris Warkentin (Peace River, CPC): I appreciate the definition of a cookie. Here we were having a discussion about whether it's what's being served at the back of the room or something different. I appreciate your definition, Mr. Geist. It was helpful for us here.

Specific groups, such as direct marketers or those people involved in the real estate industry, have raised concerns about how this might affect their businesses. There was comment in the last meeting about how this legislation may affect companies especially during this economic downturn. Obviously we as politicians are very concerned about the economic downturn and are also concerned about any group that might be affected within our own communities back home.

Of course, this has to be balanced with the interests of consumers as well. You talked about loopholes, Mr. Geist, and your concern that there may be additional loopholes. Are there loopholes that you're hearing about, or such as are being suggested to us, about which you're the most concerned? Are there any loopholes—this might be the better way to ask the question—that you think should be added or that would not alter this legislation to effectively put it in the same category you find the do-not-call list to be in?

Prof. Michael Geist: First of all, I think this is a good-news story for business, not a bad-news story. There are many businesses that want to rely upon electronic communication and have been undermined by the extent that spam has become a problem in this country. This, I think, will go a long way towards dealing with that issue. Think, for example, of the Canadian banking industry, which has invested very heavily in electronic banking only to find that the phishers have sent out a lot of messages purporting to come from the banks, which are suddenly now sending out messages to their customers warning them not to respond to these messages. That's not good for business and for the huge investments that have been made in that industry. So I think this is good news for business.

Unquestionably, there are going to be some sectors that in the past have been able to send out all sorts of messages—I think ultimately undermining confidence for others—which are going to face a problem. I believe your colleague Mr. Wallace, on Tuesday, recognized that in the context of real estate agents. If I want a real estate agent, I'll contact a real estate agent. I think specifically that when someone is selling a house, what they don't want is twenty spam messages from every real estate agent in town. That's a feature of this legislation; it's not a problem with it.

● (1625)

Mr. Chris Warkentin: Obviously you have spent some time on the task force. Did you hear from these people in the e-commerce community? Have you heard from people both in the e-commerce but also the general commerce community who use the Internet for selling other things? Did you hear any legitimate concerns that you felt should be addressed or hear of a loophole that should be included that hasn't been included in this legislation?

Prof. Michael Geist: The task force report was a unanimous report that included representation from the marketing community, from the business community, from the consumer community. We're talking about as broad a cross-section as I think you could get on this issue. It's unanimous that Canada needs to do a number of things—not just legislation, for there are other things needing doing, but legislation was a key component. It is now the last piece of the puzzle yet to be implemented.

I think what we see with Bill C-27 is consistent with what a unanimous task force report envisioned, which was broad, tough, anti-spam legislation to finally bring us up to how people are dealing with this on the world stage.

Mr. Matthew Vernhout: If I may interject here, I'm representing, combined, several hundred marketers as well. Under the policies and practices that our clients are already working within, they are collecting consent. They are falling already within the legislation, under the implied definitions or under the expressed definitions we already are seeing.

What we are looking at and what Mr. Geist has implied already is that those people who are already doing the bad things that we want to stop are undermining the channel of communications. For every legitimate e-mail you're getting, you may be getting five that you don't want. That's what we want to stop. It's the legitimate marketers who are doing the right things already, working with this law and already taking these actions.

The Chair: Thank you.

Thank you, Mr. Warkentin.

Before we go to Monsieur Vincent, I want to let committee members know that this morning the clerk e-mailed you the task force document titled *Stopping Spam: Creating a Stronger, Safer Internet*. The task force reported in May 2005, some four years ago. In the back, the document has a very good glossary of definitions of these various terms, such as “cookies”, “SMTP”, “http”, “SMS”, and all these other words that you're probably wondering about. I encourage you to read it and refer to it, because I think it's quite good. It's the document Dr. Geist just referred to.

Monsieur Vincent.

[*Translation*]

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

Welcome to all.

In your presentation, Mr. Geist, you mentioned real estate scams. I would like you to elaborate on this aspect. I would like you to tell me what the issue is in this regard.

[*English*]

Prof. Michael Geist: The concern is that there are any number of subject matters that you find with respect to spam. The presentation referenced some of them, whether it's body part enlargement or otherwise. But fake real estate scams, property in some country, are included in that list. People send out spam messages, preying often on seniors and others, to suggest that they have a once-in-a-lifetime real estate deal, in the hope that they might lure them in.

My concern here was to recognize some of the concerns that may have been expressed from some in the legitimate real estate community. I'm not trying to suggest in any way that anyone involved in the legitimate real estate community is sending out these messages, but simply that if there is any thought of carving out that notion of real estate, you have to be awfully careful, because suddenly you're opening the door potentially to full legalization for what is a known area for fraudsters to operate in.

Mr. Matthew Vernhout: There are also scams on things such as “Craigslist” around apartments for rent. They'll have a too-good-to-be-true, large apartment for rent at a very affordable price. People will send first and last months' rent from out of city, show up, and there's no apartment. This is something else that supports the idea behind real estate kinds of scams that are perpetrated on the Internet.

[*Translation*]

Mr. Robert Vincent: Let me go back to software. If I buy detection software, such as that from Norton, for example, I will own a license contract. Every month, I will receive an e-mail telling me to download the new anti-virus updates. If I understood correctly your presentation, after 18 months, this would become illegal, there would be a fine because the 18-month period would have expired.

● (1630)

[*English*]

Prof. Michael Geist: Not at all; if you have an active relationship with your antivirus provider and give them consent—because of course what you want is for them to send you updates every month, so you give them the consent, saying “send me updates every month”—and they do that, this can continue until you decide to withdraw your consent.

In talking about the 18 months, or the six months, we're talking about instances in which you haven't provided consent; instead, what we are doing is implying that you would agree to having this sent, even though you never really said that you would. For something like antivirus software, though, surely the whole point of it is having regular updates as new viruses emerge. Surely the consumer is going to consent to those regular e-mails.

[*Translation*]

Mr. Robert Vincent: On Tuesday, I talked about the do-not-call list. Mr. Dayman's presentation shed some light because I did not know how it could be done. It is possible to obtain the new do-not-call list that includes e-mail addresses. I also understand that affiliated programs exist. Therefore, I can obtain the do-not-call list, but since there will be anti-spam legislation in Canada, it will be possible to obtain the list of e-mail addresses and cycle them through an affiliated program, bring them back here and it would be legal.

Is there a way to stop that? Even if Canada passes legislation, if we do not have international legislation it will be almost useless, because people will go at it indirectly, through an affiliated program. Are there any other means to stop this use of affiliated programs?

[*English*]

Prof. Michael Geist: With respect to the do-not-call list, you've highlighted a big problem. You're right, the big problem is that Canadians can register their phone number on a Canadian list, but once someone exits the jurisdiction, the ability of the regulator to do very much about it is very limited. In fact, it gets even worse in Canada, because people register their numbers, the list exits the country, and suddenly you're getting phone calls back into Canada.

I've argued in a couple of pieces that Canada ought to be talking, at a minimum, with the United States about creating what would effectively be a North American do-not-call list, or perhaps even better, just some sort of mutual recognition. The U.S. faces precisely the same problem: that an operator may put their number on a U.S. do-not-call list, but somebody comes up to Canada and tries to call into the United States. It seems to me, since we share the same calling numbers, that at a minimum we ought to think about creating some sort of situation whereby Canada and the U.S. will jointly enforce, so that you can't easily escape to the U.S.

On the issue of spam, you're right again. There are jurisdictional challenges. That's why I mentioned right off the bat, from the beginning, that this will not solve all spam problems. There are still going to be people spamming from other countries. But at a minimum it's going to clean up our own backyard; it's going to address the Canadian-based, homegrown spam, and I think that step is long overdue.

The Chair: Thank you.

[*Translation*]

Thank you, Mr. Vincent and Mr. Geist.

Mr. Van Kesteren.

[*English*]

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

Mr. Geist, you're getting all the questions.

I want to play the devil's advocate just for a bit. What about mailing? Isn't that the same thing? When I open my mail on Friday afternoon and get a great wad of stuff that's unsolicited as well, what's the difference as far as the receiving is concerned? I know that whoever does the advertising pays a fee, but is the only difference the fact that they pay a fee for it?

Prof. Michael Geist: You say it's the only difference as if that's a small thing; it's an enormous thing. First off, there is the ability, in some instances, to ask to not receive certain unsolicited “real space” mail as well, although admittedly, lots of it still seems to make it through the door. There is a huge difference, because in the case of direct mail, physical marketing, the costs are being borne by the sender, and those are sizeable costs. They are not going to send out billions of pieces of paper, because the cost is too great, for a very low return. They really require some kind of legitimate return.

In the case of electronic messages like spam, it actually flips: the cost is almost costless from the perspective of the sender. Indeed, as they use things such as botnets and the like to send out their messages, in many instances it truly is costless. We bear the cost.

We bear the cost sometimes just in delayed time, but it's more than that. Our Internet service providers almost uniformly subscribe to various filtering services, costs that are ultimately borne by the consumer. Almost all network providers have to maintain additional equipment just to deal with the excess spam that isn't the legitimate stuff. We ultimately pay the price.

And it's not just network providers. Think of the schools, think of the hospitals that set up their own networking infrastructures, which at the end of the day are being forced to pay for this. I'd argue it's not an “only” here; it's a pretty significant cost that's being borne, and it's a clear cost shift from the person doing the marketing to the person who's on the receiving end, even though they never ask for it and in many instances don't want to have anything to do with it.

● (1635)

Mr. Dave Van Kesteren: But really, the cost factor is the only difference.

Prof. Michael Geist: Well, it's not the only difference; it's one reason there needs to be some action here. But there are other areas too, and in some ways they are related to cost. Think again about the success rates that are needed. Almost any legitimate business, if we're going to talk about businesses, is going to need some kind of reasonable return rate in order to enter into the venture. If no one ever comes into my store, the store is going to go bankrupt. If no one ever responds to my physical marketing, or if I get a very low return rate, I'm going to stop that marketing.

That's not what happens here. Here, you can send and send and send. You just need to grab that one person, that gullible senior citizen who gets this message and is told that someone desperately needs help and there's a pot of gold at the end of the rainbow, and suddenly the life savings are gone. We laugh, because we wonder who is ever going to be silly enough to fall for this, but people do. We haven't had the legislation in place to deal with these kinds of scams, much less the unwanted marketing, now going on for years.

Mr. Dave Van Kesteren: I'm going to give you an opportunity to explain something, because I have to get this straight. When I saw the notice the other day, I thought, “Oh, shoot, Michael Geist is here, and really, he doesn't like this legislation too much”, and I thought, of course, of copyright.

Is there a parallel there? I'm just asking, and I want you to explain it. Isn't the spirit of the law the same thing? We take something like a disk, and it becomes our property, and we can use it over and over again.

I think you must be somewhat of a libertarian. I am, and I like that. But I just have the difficulty of marrying the two or not marrying the two here. Isn't there a freedom of expression in our having this system? Isn't the problem the fact that we don't have something in place to charge people for pushing that stuff through the wires?

Prof. Michael Geist: I think you asked me the same question when I appeared before you in the ethics committee around the Privacy Act. So it's not always about copyright with me.

Some hon. members: Oh, oh!

Prof. Michael Geist: In this instance, I really don't think there's a parallel. What we're talking about here is, in some instances, clear criminal activity. It's activity that undermines the confidence in the legitimate market for many Canadians, and the extent to which it arises.... The only copyright connection is with respect to the Sony rootkit case, where there was that spyware, that stuff that was put into somebody's computer. That's an area where there was a bit of spillover from copyright.

But copyright, as we all know, is complicated; there are interests from the user's side and the creator's side and the industry's side, and we're trying to sort out that balance. There isn't really a balancing act here, when we're talking about scamming e-mails that are preying on individuals, or spyware that takes over your personal computer and uses it for all sorts of nefarious purposes.

Mr. Dave Van Kesteren: You won't argue, of course, that copyright...that when you take something like that, it's criminal activity as well.

I'm just having a problem with that part of it: the view that this is free, this is something that we've developed, and if you have the ability and have the opportunity to use it, go for it.

Prof. Michael Geist: I think that misstates my perspective on copyright. My perspective on copyright—and hopefully we'll have a chance to talk about copyright sometime down the road too—and I think the view of tens of thousands of Canadians who have spoken out on this issue, is that it's not about a free-for-all. It's rather about a fair-for-all and about striking the right kind of balance.

In fact it's about, when somebody does buy a CD or a DVD, that becoming their property, and their having a certain ability and right to use it without its being locked down or their being labelled a criminal if they want to play it on their iPod or want to display it in a classroom, or a range of other kinds of activities.

I don't think those who are arguing for a fair copyright are arguing for another free-for-all, Wild West online. Actually, I think they're arguing for staying truer to the notions of balance within copyright.

I want to see rules that apply online too. I want to make sure they're balanced and fair, so that we can see the kind of innovation that takes place today from a technology perspective as well as the kind of creativity that we see taking place using these kinds of tools, using nothing more than this to speak out and engage in all sorts of exciting things. That requires some rules. It just requires rules that don't try to lock everything down.

● (1640)

The Chair: Thank you very much, Dr. Geist.

Madam Crowder.

Ms. Jean Crowder: Mr. Chair, this may be a question for both the panellists. It's a question around the economic costs.

What we often hear and what I've been hearing is that there's a cost to business, if we put this anti-spam legislation in. We recognize that spam costs businesses in terms of anti-spam software and those kinds of things. But I wonder whether anybody has taken a look at the productivity costs for a business, because depending on the complexity of a task, I know from some previous work I've done that when an employee is interrupted in their work, it can take anywhere from seven minutes to half an hour to get back to the same level of complexity they were at in the task.

Has anybody quantified that kind of cost to business of the spam that's hitting people's desks?

Mr. Matthew Vernhout: I don't have the numbers with me, but yes, there is a justified cost to what spam will cost a business, and it's somewhere in the range of $300 or more per year per individual employee, as an overall cost to businesses.

That includes additional hardware, it includes lost time from hitting the delete button or hitting the report spam button; it includes the productivity loss. It also includes just the infrastructure needed—extra bodies of support for that infrastructure, if you need an additional IT resource, or something like that. So there are justifiable costs.

Ms. Jean Crowder: Has anybody taken a look at what the number would be of the cost to business for implementing Bill C-27?

Mr. Matthew Vernhout: I don't know what the number would be, but I would think it would be relatively small to say, “You have given us consent to communicate with you”. In many cases, it's a database update that takes five minutes on your website to say, “Check this box. Now you've given us consent”, or “Reply to this e-mail to say you've given us consent”.

Ms. Jean Crowder: Many marketers already do that. You sign up for stuff and—

Mr. Dennis Dayman: That's the point I was going to make. A lot of them are already doing this today from a best practices standpoint. My experience in the U.S. with CAN-SPAM, when we were working on the law back in 2003, was that a lot of concerns just like that were brought up, and what we have found out over the last several years is that being in this business has now become a bit easier, because now we have a better grasp on the data flows that we have, either in our own companies or from what other marketers are doing today, because they're doing the right things. They're basically flipping the model from quantity over quality to quality over quantity, when it comes to data that's coming in—the opt-in aspect of it—so we have found that it's much better for us right now.

Ms. Jean Crowder: That would make sense. I think legitimate businesses that are already practising good marketing techniques with regard to spam have already developed the technique, so it shouldn't be a huge cost to other legitimate businesses to adopt something that's already out there.

Prof. Michael Geist: I was just going to say that I find it amazing that more than ten years after we introduce private sector privacy legislation we're still acting as if obtaining appropriate consent from their customers is something new for business. I mean, please.

PIPEDA, the private sector privacy legislation, was introduced in 1998. It didn't take effect until several years later. We all thought that would provide everybody with plenty of time to get used to this, just as with the do-not-call list, and now with this. Businesses have been operating in an environment where obtaining the consent of your customer has been in place for the better part of a decade. Making sure that your customers are agreeable to hearing from you is not something that is so new.

Ms. Jean Crowder: I have a quick question on enforcement, as I'm running out of time here.

I know there are the hefty fines and all that kind of stuff, but are the enforcement provisions in Bill C-27 adequate? In your view, are there enough funds around resourcing those enforcement measures? Oftentimes in legislation we put the enforcement mechanisms in place but then we simply don't resource them.

● (1645)

Prof. Michael Geist: I can't answer the resourcing question because I don't know how much money has been allocated.

Ms. Jean Crowder: That's a question for the minister.

Prof. Michael Geist: I do know that one of the recommendations that came out of the spam task force was on the resource side. One of the barriers that we consistently encountered was that there were agencies or enforcement agencies that were willing to take action, or said they were willing to take action, but there was a resource problem.

Are the enforcement provisions deficient? I think on paper they are. I will tell you that throughout the process of the anti-spam task force, we consistently looked for action from some of these enforcement agencies, and frankly we had a hard time getting it. In fact it hasn't come up, but I launched the first anti-spam privacy complaint under PIPEDA with the Privacy Commissioner's office. It was a successful complaint in the sense that it was found to be well founded, but it didn't really get much further than that.

I realized from that, and I think other people realized throughout that process, that it's going to take a clear mandate so that enforcement agencies understand that this is a priority of government. It became very clear that the way you do that is you pass legislation that really targets it, and then you resource it appropriately. That's clearly what Bill C-27 is trying to do.

The Chair: Thank you.

Mr. Brown.

Mr. Gord Brown (Leeds—Grenville, CPC): Thank you very much, Mr. Chair.

I want to thank our witnesses. This is actually quite interesting.

As a business person, I am keenly interested in what you touched on a little bit, Professor Geist, about how this is actually going to be a benefit to business. I know, and I've already had some business organizations talk to us about how they fear this will be a negative thing for business.

All of you could get in on this and explain just a little more why business shouldn't fear this and how this will actually be a benefit to them.

Prof. Michael Geist: I'll give you some views from my perspective and then pass it over.

I think we've recognized and been talking for the better part of a decade as well that electronic marketing represents a huge opportunity. It is obviously lower cost. The one thing we have seen happen over the last ten years is this huge migration of the public into the online environment as well. So I think everybody recognizes that this is a great way to go. It seems everybody but the newspapers were happy with this. The newspapers weren't so happy, of course, because we are moving into this online environment more and more. So it's obvious that there's great commercial potential there.

I think not just in this country, but particularly in this country, given the absence of legislation, the potential and the promise of using electronic marketing has been undermined by consumer confidence, by the amount of spam that you get and the overzealous spam filters that weed out legitimate mail from the illegitimate mail so you never actually get the messages that you want to get. You get people who ignore just about anything that's commercial, because suddenly they think it's all that spam stuff, even when it's something they might otherwise want to hear about—for instance, when the banks have to warn their customers to ignore the messages that purport to come from them, because they're not going to send those messages. That's harmful. That's harmful to a bank, clearly, but it's harmful generally to businesses who see a real opportunity and who in many ways might have a customer base and a demographic that would respond to electronic messaging yet are facing an environment where there's just a flood of the unwanted stuff with no way to try to stop it.

I think for those who are doing legitimate business, this is really going to be a ray of sunshine, where suddenly now there is an opportunity to legitimize this form of marketing.

Mr. Matthew Vernhout: I would fully agree, and that is something we have experienced working with both direct mail marketers and electronic mail marketers. There is a significant shift because of cost, especially in a down economy. People are looking at how they can save their budget. Online marketing budgets are getting larger. Offline marketing budgets are starting to shrink accordingly, because of the cost, because of the return on investment.

The Direct Marketing Association saw a $45 or $48 return on investment for online electronic e-mail communications with consumers, so what you're seeing, even with the direct mail piece, is that if you send 10,000 messages and 100 people respond, that is considered successful. If you send 10,000 e-mails and 100 people respond, you've failed at what you're doing, because the response rates and the interactions of people are such a significant thing that businesses are relying more and more on electronic commerce because of the cost, because of the cost savings, and because of the high returns and the measurable, tangible results, which they can see through how many people are opening, how many people are buying, and how many people are interacting with their messages. There are the tangibles that will help business in this regard.

Mr. Dennis Dayman: Just to add to that, I was saying earlier that, at least in America with the CAN-SPAM Act, we've seen improvements in marketing. From Eloqua's standpoint, it is the same thing. Especially in this down economy we've seen people go from the postal side to the online side mostly because it is cheaper, but we've also found we can send a more relevant message to people. We can better segment people so we can say that this one group of people have not gone as far into the buying process or the education process of buying, let's say, anti-spam software, whereas this group might have, so let's send them kind of a different message. Let's send them a more targeted message so they are happier. They're unwilling to unsubscribe or complain about it, and again, you're continuing to educate this person, so, again, you get a better understanding of what is really going on in your marketing and sales groups now versus just batching and blasting out the same postal mailer over and over and wasting your time with it.

● (1650)

Mr. Gord Brown: All right. Thank you for that little enlightenment on how we can help reassure some of the businesses that are concerned about the impact of this.

I'd like to get a little bit into this spam reporting centre and the understanding of what the mandate for that would be, how it might work, and what might be the best model for that to coordinate this whole effort.

Prof. Michael Geist: My view is that it is an issue that has evolved. At the time when we were on the spam task force, the Federal Trade Commission spam centre—fridge or freezer or whatever it was called—was seen as a useful tool for investigative purposes, and there was the sense that we ought to create a Canadian equivalent. I think it was the fridge, and we were going to be called the freezer. Today I'm not sure that is as necessary, but what I think is necessary is empowering Canadians generally with something to do. I get this a lot in some of the other areas I'm involved with. People get these spam messages. They know there is spam legislation out there. They want to do something. Creating a spam reporting centre that can engage in some analysis and that can actually track incidents of spam and perhaps try to identify where some of those Canadian sources are would be of some value.

To give the parallel on the do-not-call situation, in my office I have literally 2,000 pages obtained under access to information that show four months' worth of the complaints that have been filed with the CRTC under do-not-call. They go by date, and you can actually see the telemarketing campaigns as they wave through the country. All of a sudden, over a week, you will get—I won't bother naming the companies—a particular company about which there are suddenly dozens of complaints in a segmented time. That could be very valuable to someone for investigative purposes if we were dealing with something that was illegal.

Creating that kind of spam reporting centre has some of those benefits and also gives people a bit of empowerment in terms of having something they can do when they receive these messages.

The Chair: Thank you, Mr. Brown.

Before I go to Mr. Rota, my understanding is that 70% to 80% of all SMTP traffic over the Internet in Canada is spam.

Prof. Michael Geist: We have even higher numbers.

Mr. Matthew Vernhout: I would say what you're seeing is over 90%. I believe there was a study that came out last year that said it was 95% of traffic, and even the difference of a 1% increase represents billions of messages, as opposed to thousands, so the significance of a single percent of increase is very huge.

The Chair: Thank you.

Mr. Rota.

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

Thank you for being here today.

I'm looking at the areas of resourcing and enforcement of the law. In 2002 the Utah legislature passed an anti-spam bill in an attempt to stem spam from being in the inbox of its citizens. The law classified spam as unsolicited e-mail sent to someone who was without a prior business relationship with the company, and the definition is very similar to that in Bill C-27, from what I understand. In their bill, they provided for a right to civil action for violation, much as clauses 47 and 51 of Bill C-27 do. Any spam sent to a person gave that person the right to file a civil suit against the company.

Although damages were limited to $10 per e-mail, the law also allowed for attorney's fees to be paid if the spam recipient was successful in court. Utah's anti-spam law resulted in a flood of anti-spam suits in the court. By the end of 2003, two Salt Lake City attorneys had filed more than a thousand lawsuits under Utah anti-spam law against companies such as Verizon, eBay, and Columbia House. These are clearly larger corporations.

In December of 2003 the U.S. Congress passed the federal anti-spam law, the CAN-SPAM Act, which trumps the state law, and in 2004 Utah's anti-spam law was repealed, but not before the Utah courts were basically clogged with anti-spam lawsuits. Many legal experts have said that it was because of the civil action for violations that this particular law was struck down.

That concerns me when I look at our legal system, and how backed up it is. When I look at this, I see this mad influx of civil lawsuits against companies that normally wouldn't be sued and that seemed to be doing the right thing. As Bill C-27 includes that private right-of-action clause, how do you see this affecting our legal system?

● (1655)

Prof. Michael Geist: As I mentioned, I recognize the potential for parallels, but I actually don't think that the concern within the Canadian legal system is as great. As I mentioned, there are reasons for that, including the fact that it is tougher to even get a class action status in Canada than it is in some states in the United States. There are court costs often to be paid in Canadian actions that are not paid, in terms of the losing party in Canada, and that doesn't exist in the United States. So we have some disincentives already in place in Canada against these kinds of frivolous lawsuits.

I would note, though, that in a Canadian context we have had—and it was stunning, frankly, to me as a member of this spam task force to learn this—a series of large Canadian-based spamming organizations. We knew who they were, we knew where they were, and yet we weren't doing anything about it. And we also knew that there were organizations out there that were anxious to try to launch private actions against them and felt that they couldn't do so in Canada.

The private right of action was a recommendation, as I say, from the unanimous spam task force report, which included some of the same kinds of members you've just referred to. The business community was there. I think we had members who came forward and said if they had that kind of power here, they might do it. If you refer to the Facebook lawsuit that was brought up earlier, you'll see that Facebook sees a Canadian-based spammer that's wreaking havoc on its social network. Canadians are huge users of Facebook—there are more than seven million Canadian-based accounts on the Facebook network—and yet they couldn't look to Canadian law to try to deal with the problem. Private right of action holds the promise of doing that.

Mr. Anthony Rota: For clarification, you're saying that they would only be able to sue for damages?

Prof. Michael Geist: What I'm saying is that I don't anticipate the flood of lawsuits in Canada, in part because our court system is somewhat different from that of the United States. The fact that Utah was a leader in this regard isn't by accident. There was a very well-known spammer who was Utah-based, which is why the state felt that it was incumbent upon them to try to take action. You had other states that were of the same view, and then Congress jumped in to say okay, we're going to try to pre-empt all of those state laws, because now we're getting this patchwork, and that's making it difficult for business.

If there was a concern around spam laws at that time in the U.S., it was more that businesses were being faced with different regulatory systems in different states, not with the notion of complying with some sort of basic anti-spam legislation.

Mr. Anthony Rota: Lawyers can act on contingency in many provinces in Canada. That's pretty well the same anywhere. When you have lawsuits that go up to $10 million, that's a heck of an incentive for individual lawyers.

Would we be better served if it were the state that imposed that fine, rather than having individuals filing civil lawsuits, as far as fining goes, for people who break the law?

Prof. Michael Geist: I think the legislation already includes.... There is an enforcement arm. The goal of the task force, I assume, by virtue of this legislation, was to try to find a number of tools to go after this.

Certainly there is within this legislation, as you know, a number of enforcement agencies that can go after spamming activity. It can result in pretty sizable penalties. I'm not about to go out and launch any of these lawsuits, but we heard consistently from certain businesses who are deeply affected by this that if we had a private right of action in place, they'd be inclined to try to use it. In some instances, they grew so desperate about the Canadian situation they filed suit, but were forced to do so elsewhere.

The Chair: Thank you, Dr. Geist.

Thank you, Mr. Rota.

Mr. Lake.

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

I'm going to just revisit the business side of things and the cost of doing business.

Prior to getting elected in 2006, I worked for the Edmonton Oilers hockey club. At one point, I was the director of ticket sales back in the late nineties. I thought it would be a good idea, as director of ticket sales, to post my e-mail address on the website. People would e-mail requests for season tickets and I could pass them on to the sales staff.

It didn't turn out to be such a great idea. I got a tremendous volume of many of the types of e-mails you've talked about. Of course, this was back in the days before we had the spam filters to the extent that we have them now.

In the end, I had to eventually change my e-mail address and of course change all my business cards. All the people who would have had my e-mail address couldn't use it any more. They couldn't reach me, because there is no way to fix that. I couldn't just have the e-mails forwarded, because I'd get all the spam again, right?

We had to hire an extra staff person to clean up the spam. I remember we had to invest some fairly significant dollars into technology software to filter out the spam. If you multiply that cost business by business, across the country, you start to see some pretty enormous costs of doing business.

That's enough said on that. That's a little bit of a speech, I guess.

Do you have a sense of how high the cost is to business?

Maybe I'll give the fellows on the right side of the table a chance to answer that. I sense that you do have some numbers you can attach to this.

● (1700)

Mr. Dennis Dayman: Yes. I was actually taking a look at a statistic I did a couple of years ago. Back in July of 2004, the United Nations actually estimated that spam cost the global economy around $25 billion annually. Obviously since that time it's heavily increased.

That's one of the numbers I've been able to work from.

Mr. Matthew Vernhout: I would imagine it's double now—

Mr. Dennis Dayman: It's way higher now.

Mr. Matthew Vernhout: —if not more than that, mainly because of the industry, almost, that came up to prevent spam. People have heavily invested in it, and the services are not cheap. The price for some of these services is somewhere in the area of $50 a month per mailbox. If you times that by 10,000 employees, that's a pretty hefty anti-spam bill you're fighting annually.

Those types of services and costs are based not only on what it costs to prevent spam but also on what it costs in employee time. We had briefly touched on that earlier with one of your colleagues. It would cost easily $300 a year per employee for just the time it takes to hit the delete button or to move it to a junk folder. That's significant time that you're breaking someone's work flow.

Mr. Dennis Dayman: Yes.

If I may, Jay Thomson, the former head of the Canadian Association of Internet Providers, estimated that the average cost to consumers was $5 a month. That cost that has since jumped up.

What's interesting, though, is that the amount of spam you see today in your inbox is probably only 10%. The other 90% is actually being taken care of either by the government or by Hotmail or whatever organization that hosts your e-mail. So you can imagine the amount of e-mail that's coming in.

AOL, about four years ago, noted that they had blocked about half a trillion messages. That was only four years ago. Again, we would look at that and say it's probably doubled, if not tripled, to that extent. Once you start adding in that $5 on their side of it.... It's going up.

Mr. Mike Lake: It's funny hearing you illustrate some of the problems, because even as a consumer, sitting at home, I get these pop-ups that come up and say that my anti-virus software is out of date, or that my Windows needs to be updated. I don't even automatically do that any more, because I'm worried that someone has sent me something to look like Windows or look like the anti-virus that I might be putting on my computer.

I think I actually know a thing or two about computers, and I'm uncertain about this; I can't imagine how difficult that makes it for someone who is a newer user.

Prof. Michael Geist: I think it's almost impossible to overstate the effect that this has on consumer confidence.

I can recall, actually, that when we launched the spam task force, there was a press conference. I remember one of the reporters turned to the task force members and asked—I happened to be the one who responded—what would make this a success. I noted that when e-mail first arose back in the mid-nineties, people started popularly using it. You used to follow up with a phone call to make sure that the person got the message. Then there was a period of time when we stopped doing that. We just assumed that the message had been received.

We're back to making that phone call. If you don't hear back from the person within a day or so, you almost assume that you either have to pick up the phone or re-send the message because it's been caught in the spam filter. It has rendered what is otherwise an exceptionally important tool for communication into one that is simply not reliable any more.

Mr. Mike Lake: I have a last question. I think my time is almost up. If I could, I would like to close with Dr. Geist.

We're in a minority Parliament situation. Time and time again, we've seen legislation come up, good legislation, that winds up not passing through the House and the Senate before you get an election. Who knows when we might be headed to an election? Hopefully it's three years from now, but I'm not holding my breath until then.

What is the importance of getting this legislation through and not having it die with a parliamentary dissolution?

Prof. Michael Geist: It's taken four years to get from the point of a unanimous task force report that included everybody across the spectrum to finally just getting legislation tabled, and there were a couple of false starts along the way. The notion that we're going to go back to zero I think would be enormously problematic, particularly at a time when we've seen, from across the spectrum, all parties—this is clearly a bipartisan issue—industry, and consumers saying that Canada is quickly falling behind from a digital perspective. We need a digital strategy, otherwise we're going to fall further and further behind.

From my perspective, this forms a part of that digital strategy. And if we're unable to see this get through, and get through quickly, it represents a setback not just for this particular piece of legislation but for the larger Canadian digital environment more generally.

● (1705)

The Chair: Thank you, Mr. Lake.

Monsieur Bouchard.

[*Translation*]

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

My question is for Mr. Geist. You stated that legislation is effective when there are penalties. If I understood you correctly, without penalties, enforcement is just about nil or in any event weak.

Are you happy with the penalties included in Bill C-27? What can you tell us about the penalties under this bill?

[*English*]

Prof. Michael Geist: As I think we've mentioned, the experience elsewhere is that unless you have strong penalties, this doesn't work. I think there were even some quotes in the press from one Canadian-based spammer, who was laughing when told about the prospect of Canadian anti-spam legislation and indicated they figured they could just keep on going.

There's obviously a certain kind of profitability that a spammer or a fraudster is going to have. The only way to counter that is to make the risk far greater than it is today, that there are real financial penalties at stake. This legislation has that.

We keep bringing up Australia, but Australia is the one place where they brought in penalties that at the time were seen as unprecedented. The reports coming out of that country were that many of the spammers were either picking up and going elsewhere or finding a new line of work. It really did have the effect of increasing the risk of engaging in that business to the point that they went and did something else or did it somewhere else.

[*Translation*]

Mr. Robert Bouchard: Mr. Chairman, I am going to share my time with my colleague. But first I would like to ask another question.

Let us talk about coordination. Three agencies have a role to play under Bill C-27: the Competition Bureau, the CRTC and the Privy Council. When the minister last appeared before the committee, he told us that a coordination agency would be set up and that it would not be very large. I would like to hear your views on this. You mentioned that each organization should have a specific mandate. I understood you to say that it will be important to assign a clear mandate to each organization. Is Bill C-27 clear enough in terms of coordination?

[*English*]

Prof. Michael Geist: There are provisions that discuss that ability for information-sharing and coordination between agencies. Obviously the provisions themselves, in some instances, are targeted to a specific agent, one or the other, and one would hope that, properly resourced, there will be the ability to carry out that mandate. And as I mentioned, the fact that this legislation will come, and one would hope would come in a unanimous fashion from the House, from across all sides, I think sends the strongest signal possible that this is a priority and the time to act is now.

[*Translation*]

Mr. Robert Bouchard: Thank you.

Mr. Robert Vincent: Mr. Geist, I have a question for you. This bill will truly change the way many people work. During this discussion, an example came to my mind. Suppose I tell you that my house is for sale and I ask you if you know anyone who might want to buy it. You could answer that one of your friends is a real estate agent. You will talk to him about it and he will send me an e-mail. I would never have talked to the agent himself, because he is your friend and not mine, so I would not know him. In such a scenario, he would contravene the law and could get fined.

Is there something we could do in order to allow these people to continue working effectively through the Internet as a useful tool?

● (1710)

[*English*]

Prof. Michael Geist: I think there are still a lot of options in this regard. In fact, when I'm asked to make a connection with someone in this kind of context or other sorts of contexts, my approach, partly because I'm concerned about the privacy of the individual, is to send the person who's made that request the contact information and say, "You ought to contact this person." I often might send a similar e-mail to the person who they might be contacting, saying, "Keep an eye out for a message from my friend who might be contacting you."

In that case, the person who wants to make that connection with the real estate agent is making the contact directly. There are no issues whatsoever. I actually think that's the healthier way of approaching this. I'm not handing out my friend's e-mail to all sorts of commercial entities. Instead, the person is able to contact them directly.

Of course, there are still other ways to market or to get that initial consent from that individual. That real estate agent can pick up the phone, assuming the individual is not on the do-not-call list, and make a phone call if they want. However, because we've seen people's personal information misused at times, I think the better approach in terms of how we make those kinds of business connections is to actually put the control in the hands of the individual who wants that service. Let them reach out to your real estate agent and let me provide them with the information they need to be able to do that.

[*Translation*]

The Chair: Thank you.

Madam Coady.

[*English*]

Ms. Siobhan Coady: Thank you.

I want to talk to two issues. One goes back to Mr. Lake' s point about having his e-mail address on the web. I was CEO of my company and I had my e-mail address on the web; luckily, it went to a different box than my inbox. That is a concern for this particular bill as well, and I think Bill C-27 should look at it. We have a lot of precedents around the world, so we can draw on the best approaches.

To go back to Mr. Lake's point, I'm going to draw your attention to a case in New Zealand. New Zealand had an issue when they had their school addresses published on the web, which is a very common occurrence here in Canada. They ended up having a challenge. E-mails were being sent from businesses offering them goods related to education and they weren't being allowed to go through. The ministry added a note to the web page saying that the addresses could not be used to send commercial electronic messages. Are you familiar with this?

A voice: Yes.

Ms. Siobhan Coady: Okay.

New Zealand put it on the website that they could not send commercial electronic messages and that got around this. Bill C-27 hasn't addressed that. Do you think there's something that we should be doing in this regard? It would capture Mike Lake's point about having his e-mail address published. Also, on Facebook, your e-mail addresses are published.

Prof. Michael Geist: Well, I actually think the legislation does deal with this in part, because there is, as I mentioned, the business-to-business exception. I'll tell you that when I launched my spam complaint, it also happened to be against a sports team. It was against the Ottawa Renegades, the old CFL team, not that they were spammers, but they kept sending me these messages. They lifted my address off the university's directory.

I found it interesting to note that the university took the position that this was the university's commercial e-mail address. Now, there is an exception for true business-to-business e-mail, where it is directly related to the business itself. If someone was trying to send Mr. Lake a message that was about a hockey trade, tickets, or something like that, that's directly related, and you're okay. When they're trying to sell something else entirely, the business-to-business exception doesn't apply and that would be a violation.

I actually think the law does a pretty good job, especially when we're dealing with businesses and publicly available addresses, of trying to address the instances when there is legitimate business-to-business e-mail, which can continue to happen, as opposed to the spam or the outside messages, which would now fall into the spam category.

Ms. Siobhan Coady: So having one's e-mail address published on the Internet does not fall under the consent that is “express or implied”?

Prof. Michael Geist: No. There's been an ongoing issue in Canada as to whether or not e-mail addresses are themselves personally identifiable information. At a provincial level, there actually have been some attempts to exclude that, but federally, until we change the law, they are treated as personally identifiable and thus subject to the same kinds of privacy protections as other personal information.

Ms. Siobhan Coady: I'm going to move to consent provisions again, similar to what I started talking about an hour and a half ago.

One of the concerns that keeps getting raised to me is that the consent provisions for the anti-spam prohibition are narrow. I'm going to look at what was adopted by PIPEDA and quoted by the anti-spam task force. It defined implied consent much more broadly than the legislation currently does. It says:

> “...where consent may reasonably be inferred from the action or inaction of the individual." This covers situations where intended use or disclosure is obvious from the context....

What I'm reading in this particular bill is much more narrow than that. When I look at instances—for example, the Australia Spam Act, or the New Zealand spam act—that actually define consent to include express consent or consent that can be inferred from the conduct and business and other relationships without limiting the circumstances in which such consent can exist, then I'm concerned that we're a bit narrow in this bill. Can you just give me some assurances?

The anti-spam task force again recommended broader exceptions. For example, it said on page 44:

> If the organization has service, warranty or product-upgrade information, or if there are health and safety issues related to the product purchase, the organization may send e-mail messages to its customers.

As I read Bill C-27, it doesn't do that.

● (1715)

Prof. Michael Geist: I'm going to repeat this. As long as you understand that there's a huge, massive exception, get consent. All of this is permitted as long as you obtain consent. We are now only in that basket where someone hasn't actually obtained the person's consent in the first place. They don't really know whether the person wants to get this information. In every other instance where the person has actually given them consent, it's fair game, and they can do whatever they like. So we're only in that particular basket.

The question is whether in that basket this is more narrowly constructed than PIPEDA, and the answer is yes. I would argue that is an absolutely good thing. What we have seen not just here, but in other countries as well where you adopt what is effectively an opt-out approach—one where you can imply consent in a broad number of situations—is that doing so opens you up to a torrent of potential abuse and misuse of what is seen to be consent. Here's where the rubber hits the road. When we went to various enforcement agencies and said we wanted them to take on a case, they were only going to take on a case that they thought was a slam-dunk case. If there was any kind of doubt about this, they were worried about taking that kind of case on.

Leaving aside the fact that we have this big huge honking “express consent” that covers everything, if you expand that so that almost anything is “implied”, you're going to hamstring the regulators and enforcers who are going to look at this and say the other side is saying “we think we could have implied consent in that circumstance” and you're left with no action at all.

The Chair: Thank you, Dr. Geist, Madame Coady.

Madame Crowder.

Ms. Jean Crowder: I have just a quick follow-up to something you had said concerning enforcement. You had indicated that in some of your other work, CRTC had problems with the do-not-call list, and you mentioned the complaint that you filed with the Privacy Commissioner. If there are already problems within these agencies around enforcing the existing legislation they're dealing with, what confidence do we have that they'll be able to do the enforcement under this?

Prof. Michael Geist: I admit that I think there's ample reason for some skepticism as to whether it will be enforced as effectively as it can be, at least on paper. I think that's one reason why a private right of action is a good thing, because it actually does allow the private sector to pick up the slack if we don't get the kind of action we want from the enforcement agencies.

I think the other thing is that one would hope that putting in the right resources and having very clear legislation would send a very strong message.

But you're right. At least with respect, in my view, to the CRTC and the do-not-call list, the track record isn't great, and once again we are putting a lot of responsibility on their shoulders to enforce this law.

Ms. Jean Crowder: I have just another quick question on the whole issue of privacy. You mentioned the cross-border issue and the notion that it would work best if Canada and the United States worked together. What are the privacy implications for Canadian citizens if we go that route?

I assume that the Canadian Privacy Commissioner would have to share information with the U.S. authority concerning Canadian spammers, for example.

Prof. Michael Geist: There's the potential for that. The concern has actually been the opposite. My understanding is that there have been a number of instances in which there have been international investigations with a Canadian component, and there have been concerns as to whether or not Canadian authorities could cooperate and hold up their end of the bargain. It's been less about trying to go after true Canadian-based spammers and more about ensuring that Canada doesn't ultimately become a barrier to international spam investigations because the agencies that have certain information aren't empowered to share it with their counterparts in other countries.

● (1720)

Ms. Jean Crowder: And we could deal with that through this legislative process?

Prof. Michael Geist: I think we could attempt to do that.

Ms. Jean Crowder: Mr. Dayman, do you have a comment on that?

Mr. Dennis Dayman: Go ahead.

Mr. Matthew Vernhout: I do.

Outside of the governments of the world coming together, I think you're starting to see organizations such as the Messaging Anti-Abuse Working Group, with ISPs, ESPs, and private anti-spam organizations working together to really sort of push the envelope and ask how they as organizations can raise the bar where government falls short, and how can they prevent abuse from their own networks, or abuse coming into their networks. They're really working from the business side on how we can prevent that.

With the help of government, obviously, they're going to be able to take action. What you'll see then is that the cottage industry spammer, the small guy sitting in his basement sending SPAM, will disappear. That's what Australia saw. They'll disappear overnight because they're worried about huge lawsuits.

Where you have the problem is with these large organizations. There's the Canadian Pharmacy spamming, where the Canadian organization has now moved out of Canada but still spams in Canada, still uses the Canadian Pharmacy branding, and still sends products that don't work. But there's no action. We can't do anything about it, because they've moved to other countries or they've moved outside of the borders where this stuff's enforceable because they're worried about the types of actions that can be taken against them.

Ms. Jean Crowder: Thank you, Mr. Chair.

The Chair: Thank you, Madam Crowder.

Mr. Sorenson.

Mr. Kevin Sorenson (Crowfoot, CPC): Thank you.

I'm not a regular member of this committee and am filling in for Mr. Wallace today, but it's certainly an interesting topic that you have here.

Is there a difference between unsolicited e-mail and spam? I was looking through the book that the government put out, which defines spam as "unsolicited commercial e-mail". But going back to the question Mr. Vincent asked in regard to a buddy that has something and he knows another buddy, would you say that's spam? It's unsolicited.

Prof. Michael Geist: Right.

Why don't you guys answer this too?

My own view is that we often try to get away from some of these definitional issues because early on we would have some of these discussions and spend half a day talking about what your definition is. It wasn't particularly productive, because the real focus was on where the harms are and what kinds of standards we want to set for what's acceptable and appropriate commercial marketing.

The legislation is obviously focused exclusively on the commercial side, and there's good reason for that from a constitutional perspective, I believe, but in terms of trying to ask if this is spam or unsolicited commercial e-mail, you could get a dozen people in here and everyone would give you a different answer in terms of how they define it.

Mr. Kevin Sorenson: Well, let's put it a different way, then. If I'm selling something, not as my business, or not as how I would earn my livelihood, but just selling some used product—a boat—and a buddy said the same thing Mr. Vincent said to a friend, and I then sent him an e-mail, does the legislation in any way prevent me from doing that?

Prof. Michael Geist: There is an exception in here as well for that sort of consumer-to-consumer personal correspondence. The issue is whether this now rises up to the level of clear commercial activity. I think there's some question as to whether or not it rises to that level. There is also, though, realistically, the question as to whether we are talking about any kind of real risk. I mean, is your buddy going to file an anti-spam complaint against you for telling him that your boat's for sale?

Mr. Kevin Sorenson: No, no, but my question is about the guy who's sending the e-mail. Is he going to feel that he can't even do that, that he had better pick up the phone and phone the guy, because who knows how many other calls this guy has had? Is there any way that what he is doing is contravening what this bill sets out?

Prof. Michael Geist: I don't think there are many individuals who are going to look at that and think twice before they send out a message to their friend saying—

Mr. Kevin Sorenson: That's it. I mean, it's clearly not going to take this guy who is.... In criminal law, you talk about *mens rea*, where it's a criminal intent. Obviously, the guy is trying to do a favour and has no intentions of breaking this law.

Prof. Michael Geist: Let me just give you the specific provision, because I think it will cover most of what you're talking about. It's paragraph 6(5)(a): "This section does not apply to a commercial electronic message...that is sent by an individual to another individual with whom they have a personal or family relationship...". So if you're talking about anyone with whom.... That's as defined by the regulations, so it can be a commercial message, but so long as you have a personal relationship with that person, it's outside the—

● (1725)

Mr. Kevin Sorenson: In other words, there are proper safeguards in this legislation to prevent that type of thing from happening.

I just have one other question, and I don't know if you guys are the ones to answer it or not.

A number of times we've referenced Utah. In the United States, is it state law? I know that here, all communications fall under federal law. Is it different in the United States? Does each state have different laws? Do some states have a spam law and other states not?

Mr. Dennis Dayman: There's a patchwork of laws. Typically, in the U.S. we've always kind of broken down laws almost by industry type, such as in the case of the telecommunications act and the health act. It's a patchwork either by federal law or by state law. The Utah one that keeps popping up is a state law. There are privacy issues as well. A lot of states have different privacy legislation as well to control exactly what you can do with that. Yes, there is a breakdown by state.

Prof. Michael Geist: To supplement that, it's essentially shared responsibility. You can get federal law and state law. Under pre-emption rules in the United States, if the federal law wades into an area, it will pre-empt the state law, which, as we mentioned, is what happened when they brought in CAN-SPAM. They had a multiplicity of different standards, and CAN-SPAM was used as an attempt to try to create a uniform standard.

Subsequent to that, we've now heard a number of states say that CAN-SPAM doesn't do a good enough job. We're starting to see state-based anti-spyware legislation and even state-based anti-spam legislation that has attempted to address what they saw as holes within CAN-SPAM. Sometimes there's been litigation as to whether or not it is a valid state law in light of the fact that there is a federal statute with CAN-SPAM. Thankfully, we don't have to deal with quite that complexity.

Mr. Kevin Sorenson: In the United States there may be many different types. Some states may have an effective law, in other states it's not as effective, and some states may not have any.

Mr. Dennis Dayman: That's correct.

Mr. Kevin Sorenson: This concept of a federal law—one suiting the whole country—is very positive, in your opinion.

Mr. Dennis Dayman: Yes.

The Chair: Thank you, Mr. Sorenson.

Mr. Lake.

Mr. Mike Lake: On the consent side of things, I'm thinking about the realtor example, because I think that is a relative example and may be a legitimate concern for some folks.

To clarify—and maybe you can give me your understanding of this—if a realtor asks a friend for a list of ten e-mail addresses of that guy's friends that he can e-mail looking for a potential client, sending out an e-mail like that would be restricted under the legislation.

If two friends are talking, and one of them says they're in the market for a house and is looking for a realtor, and the second friend passes that e-mail address on to the realtor with the consent of their friend after asking if it's all right to pass it on and have the realtor send an e-mail or phone them, then that would be exempt under the legislation. That would be expressed consent. Even though it's not directly expressed to the realtor, it's still expressed consent via the friend.

Prof. Michael Geist: I think the realtor would be comfortable, assuming they had asked the person if they had permission to send it on to the friend.

Mr. Mike Lake: It's important to note that's not dissimilar to how I think most of us would probably handle that. It happened to me the other day. A friend sent me an e-mail asking if, since I knew this other guy, I could send his e-mail address. I didn't just automatically send his e-mail address. I sent an e-mail to my other friend and asked if he minded if I sent his e-mail address to this friend. It was about business. He wanted to do some business, but they didn't know each other directly. I think that's sort of a common-sense way of doing things. He said yes, and I fired off the e-mail, and they made contact. I think it's just sort of common sense in terms of the way we deal with it.

I have one last question for Dennis and Matthew. You made your statement, and we talked throughout very positively about the legislation. Are there any concerns, major or minor, that you have with the legislation? I don't think I've heard any yet.

Mr. Matthew Vernhout: We've had a couple concerns, and we've sent them in in separate documentation.

The first one is about forwarding to a friend. It's similar to the idea that you were just talking about in regard to introducing a friend to a product or to another individual. The way the “forward to a friend” traditionally works is that if I'm on a website, and I like the news article that Mr. Geist wrote, and I want to send it to my privacy person at work, then I enter his e-mail address and name on the form, and I type, “you should read this article” and I hit “send”. There's no clarification concerning who the original sender is because the message didn't originate from my local computer. It originated from another server, which is managed by a website.

I think the idea behind this is that if the message is delivered and the address is not kept or recorded—it's just used to deliver a link that says go read this article with my message included—then it's not really clearly defined who the sender of the message is. I initiated the message, but it was delivered through another network. That's something we have mentioned that should potentially be clarified in the act.

There's also the identification of a sender. What's clarified as an identification? Is it the logo in a message? Because if it's an image, a lot of e-mail clients block images. That's something that needs to be looked at. You can't spam-address stuff by using a postal address, by putting a clear text postal address in a message.

Regarding the idea behind anti-spam filters, there was wording around changing the content of the message during transmission. A lot of spam filters will put headers in that say “we suspect this is spam”. Those types of things need to be clarified as well.

● (1730)

The Chair: Thank you very much, Mr. Vernhout, Mr. Dayman, and Dr. Geist. Thank you very much for your testimony.

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
