HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

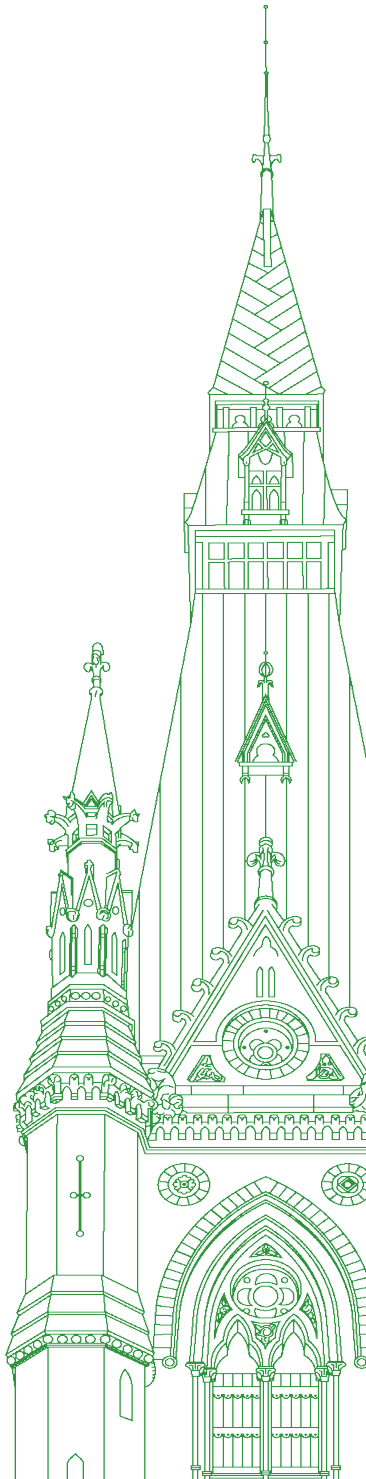
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 035

Thursday, September 29, 2022



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Thursday, September 29, 2022

● (1535)

[*English*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Mesdames et messieurs, I call this meeting to order.

Welcome to meeting number 35 of the House of Commons Standing Committee on Information and Technology.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Monday, September 26, 2022, the committee is meeting to study fraudulent calls in Canada.

[*Translation*]

Today's meeting is taking place in a hybrid format, pursuant to the House Order of Thursday, June 23, 2022.

To enlighten us today, we have the following witnesses from the Canadian Radio-television and Telecommunications Commission: Ian Scott, Chairperson and Chief Executive Officer; Stephen Harroun, Chief Compliance and Enforcement Officer; and Alain Garneau, Director, Telecommunications Enforcement, Compliance and Enforcement Sector.

Gentlemen, thank you very much for joining us today for this meeting of the Standing Committee on Industry and Technology.

Without further ado, I give the floor to Mr. Scott for five minutes.

Mr. Ian Scott (Chairperson and Chief Executive Officer, Canadian Radio-television and Telecommunications Commission): Thank you very much, Mr. Chair.

[*English*]

I want to note that we're not hearing the volume from your speaker very loudly. I'll see how it is with the other members, but it wasn't very easy to hear you speaking.

[*Translation*]

Thank you for inviting us to speak on the topic of fraudulent calls in Canada, an issue that has been of particular concern for the CRTC.

As you know, we participated in this Committee's study in March 2020, and we are pleased to provide an update on our activities.

I'm joined today by Steven Harroun, the CRTC's Chief Compliance and Enforcement Officer, and Alain Garneau, Director of Telecommunications Enforcement.

Unwanted calls, which often are fraudulent in nature, seek not only to take advantage of Canadians, but also undermine their confidence in the telecommunications system. One of our priorities over the last few years has been to better protect Canadians and prevent as many of these calls from reaching them as possible.

[*English*]

There is no single solution, no silver bullet, that will put an end to this scourge. That's why we have put in place a robust strategy that relies on a number of different technical and regulatory policy solutions.

To begin, for the past two years, telecommunications service providers have been required to block numbers that we refer to as malformed numbers, which contain numbers that wouldn't normally be part of a phone number, a simple example being 000-000 and four digits, which is obviously not a real number. They get blocked automatically so they won't get through. Alternatively, providers could instead offer their subscribers call-filtering services, which provide similar but more advanced call management features.

Callers can also act in bad faith, though, using fake caller IDs to conceal their identities and intentions, a practice known as ID spoofing, and one that has grown phenomenally in recent years. To combat that illegitimate practice, we required service providers to implement STIR/SHAKEN in June of last year, something we discussed with this committee previously. Essentially that technology will enable providers to confirm whether a caller's identity can be trusted by authenticating and verifying the caller ID information for IP-based calls, which will allow Canadians to determine which calls are legitimate and which need to be treated with some caution, kind of a red light, yellow light and green light.

We're awaiting the first annual reports from the providers, and those will help us assess how implementation has progressed and help us understand what the results are revealing to us. What we do know, however, is that many of the technical issues we and the industry were confronting have been overcome, and also, smaller providers are coming on board to provide similar protections.

Another element in the battle against these calls is artificial intelligence, which is a promising new weapon. Sometime ago, Bell Canada developed a solution using artificial intelligence to block calls that were confirmed as being fraudulent in the company's network. We allowed them to do a trial. We approved the trial and, encouraged by the results of that 15-month trial, we approved an application by them to implement that technology on a permanent basis last December. To date, that application has blocked more than 1.5 billion calls at source, and they have been intercepted. That's 1.5 billion times you didn't have to answer your phone to hear something you didn't want to hear.

[*Translation*]

The CRTC is also working with the telecommunications industry to develop a process to trace calls back to their point of origin in the network. The industry conducted a trial that yielded positive results, and so we directed providers to begin the rollout of the process toward its full deployment. The intelligence that we will be able to gather by pinpointing the origin of nuisance calls will help improve our enforcement efforts.

Of course, we continue to oversee the National Do Not Call List. Canadians have registered more than 14.6 million numbers on the list since it launched in 2008. Complaints submitted through the list operator help to inform our outreach efforts and enforcement actions.

Our ongoing work with the industry, the Canadian Anti-Fraud Centre and the RCMP enables us to exchange information on nuisance communications. We are also in regular contact with a number of federal departments and agencies, including the Canada Revenue Agency, the Competition Bureau, Employment and Social Development Canada and the Communications Security Establishment. Through this engagement, we can warn Canadians of illegitimate campaigns in a timely way to help them avoid becoming victims of fraud.

This Committee is well aware, however, that the issue of fraudulent calls is not limited to Canada.

● (1540)

[*English*]

It's not just in Canada. It's a problem in many countries, particularly English-speaking countries. In the United States alone—I think I've shared these numbers with you before—it's estimated that there is something in the order of 2,100 robocalls every second, and something approaching 50% of those may be fraudulent.

In particular, we have established formal arrangements to share information and expertise and to provide investigative support with our counterparts in the U.S., the U.K., Australia, New Zealand and Japan.

Through all of these initiatives and with the help of industry and our domestic and international enforcement partners, we are making significant progress in protecting Canadians and restoring faith and confidence in the telecommunications system.

With that said, my colleagues and I will be happy to attempt to answer any questions you may have.

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

Before we start, could you repeat the statistics you just mentioned?

Mr. Ian Scott: These change all the time. This is the U.S. statistic, but approximately—

The Chair: I think it was the number of calls per minute.

Mr. Ian Scott: It was 2,100 robocalls per second. Those are United States figures, but they're very proportionately similar in Canada. We have very similar patterns. Of those 2,100 robocalls, obviously a portion, in fact a slight majority, are legitimate telemarketing, but that means something close to 50% are fraudulent, so think of it as 1,000 calls a second being fraudulent.

[*Translation*]

The Chair: That's why, despite all these efforts, I still get a lot of these calls, and they just seem to be increasing in number.

Without further ado, I give the floor to Michael Kram for six minutes.

[*English*]

Mr. Michael Kram (Regina—Wascana, CPC): Thank you very much, Mr. Scott and the witnesses from the CRTC, for being here today.

I should start by saying thank you for all the work you have done on this file. I think there is broad consensus among all parties that reducing fraud is a good thing for everyone regardless of one's political stripe.

I read with interest the report from the last time the subject came up. Based on my reading of the report, I got the impression that you've come a long way over the last decade or so, and I think that if someone started up a fraudulent call centre in, say, Regina, which is my city, and all of its victims were in Saskatoon, I would suspect there would be a very good chance that the fraudsters would get caught. I also read that a great number of the fraudulent calls originate overseas, which brought me to recommendation number 4 in the report, that these preventative measures should be included in future and ongoing free trade agreements.

Let's start with the do not call list. Can you elaborate on how the do not call list can or should be integrated with future free trade agreements?

● (1545)

Mr. Ian Scott: We should probably start by dividing up some things, and my colleagues will assist me.

Do not call really relates to telemarketing, and we have a set of rules around it. Then we have CASL, the anti-spam legislation, and that goes to other types of communications. So we have to watch the terminology.

What do not call does is establish a system in Canada for Canadians to put their phone number on a list so they will stop being called by legitimate telemarketers. We police that, and there's a large uptake. My colleagues can give you more specific statistics if you wish. I told you roughly how many numbers. In excess of 14 million Canadians have their number on it.

There's an exemption for charities and surveys. There's an exemption for political parties, which you granted yourselves. We do get lots of complaints asking how come people still get calls from.... We will leave that alone. It is the will of Parliament, and that is fine, of course, but that's not the problem.

The problem is those who either decline—legitimate telemarketers who fail to sign up—or illegitimate ones. The first case we pursue. We get complaints. We identify them. We track them down. Either they sign up or we fine them, and we're pretty good at that, I'll be honest.

The second case is the illegitimate ones. They're not playing.... They could be foreign or domestic. That brings us into that other category, in which lots of activities are coming from abroad. What we do there is not so much an issue of free trade agreements. It's an issue of, first, establishing co-operative mechanisms with other countries, which we've been doing—and I recently revised and modernized agreements with both the United States and Australia to enhance our co-operation—and second, having initiatives like call traceback, which I referred to in my remarks, that will help us figure out where these calls are coming from.

After that, if they're coming from a particular part of the world, then we have to pursue that with foreign officials, and it goes to our enforcement partners and the Department of Justice. At that point it gets more difficult and is in fact largely out of our hands.

Mr. Michael Kram: Let's start with the United States. Is Canada's do not call list currently being shared with telemarketing firms in the United States, and is there a reciprocal agreement in place so that Canadians have to abide by American laws as well?

Mr. Ian Scott: Steven, do you want to speak to that?

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): Absolutely, and that's a really great question.

I'll go back for a little bit of clarification. Fundamental to the list is that telemarketers have to buy the list of numbers to ensure they don't call Canadians, so I think you're right. Most Canadian companies that are legitimate will purchase that list. They will not call people on that list. That's for anyone calling Canadians.

We do have American telemarketing firms that register on the list. We have foreign telemarketing companies. Last year there were, I think, 943 telemarketers registered to purchase the list. I'll do my rough math here. About 50 of those are outside of Canada, most of them in the U.S., but we also get some from the U.K. and some from Morocco. They are aware of the rules and they've purchased the list.

The same goes for Canadian telemarketing firms. They have to abide by those rules in the U.S.

Mr. Michael Kram: The recommendation in the report was that these measures be included in current and future free trade agreements, but would you suggest that other treaties outside of free trade agreements might be more effective, or what do you think would work better?

Mr. Ian Scott: I think it may be outside of our area of expertise to determine how best to do it. The way we are pursuing it is through bilateral and potentially multilateral agreements between similar agencies. The regulatory authorities in those other countries—and I recognize that our answers are going quite long. I'm sorry. I don't want to use up all of your time. I'll beg the indulgence of the chair for a second.

We will work with those agencies, and there potentially could be some room—I've been having discussions with some of our partners—to make some of those arrangements multilateral, because frankly this scourge is expanding. North America was sort of a hot spot for many years, and we see it growing particularly quickly in other English-speaking countries, but it's also growing in Asia, French-speaking countries and so on, so we're working with those partners, and that's where our focus has been.

● (1550)

Mr. Michael Kram: Thank you.

The Chair: Thank you.

We'll now turn to MP Dong.

Mr. Han Dong (Don Valley North, Lib.): Thank you, Chair.

Mr. Scott, it's good to see you.

Welcome to the other witnesses as well.

I want to quickly follow up on Michael's question. You talked about how telemarketers get their list, but what we're focusing on here are criminals and not legitimate businesses. How, technically, would these criminal groups get access to this list and constantly update the list?

Mr. Ian Scott: Thank you for the question.

I'm not correcting you, but I get corrected by my staff all the time to make sure I don't refer to people as criminals. There are people engaging in activities—

Mr. Han Dong: Suspects.

Mr. Ian Scott: —with malicious intent, but they're not criminals unless they're convicted of doing these things. I guess there's really a difference.

They're not using the list. The point is, when you get calls, whether from those using spoofed numbers or others who are ultimately engaging in fraud, they don't care about a list. They're using equipment—Alain, you can help me here—to simply randomly dial. The numbers are typically sequential. They'll sit there and say, "I'm going to dial everybody with a cellphone number beginning with 889", and then they start dialing them all.

Mr. Han Dong: Got it. The chair mentioned that since the pandemic we've seen that the number of calls, text messages and emails is on the rise. I'm really concerned about the newcomer group and more vulnerable populations such as seniors, because the callers are getting more clever. Whenever there is a new policy announced, they're very quick. The next day you get "do you want to access your CRA rebate?" or something like that, and they're very clever.

What have you done or what do you know about what the industry has done to protect the vulnerable population in Canada?

Mr. Ian Scott: That's a wonderful question. Thank you.

We do several things, and again I'll invite my colleagues to add.

I guess the first thing we do is obviously try to limit—

Mr. Han Dong: Actually, can you give the committee some statistics, maybe later, on what resources you have spent protecting specifically the more vulnerable population? I have a few more questions.

You mentioned that you work with other departments of the government—RCMP and whatnot. I don't expect you to answer as to the resources they have dedicated to fight fraud calls, but how much has the CRTC and the telecom industry spent on an annual basis to fight fraud calls? Do you know if there's a number?

Mr. Ian Scott: I'll try to answer the two questions if I can.

First of all, our focus is obviously attacking the problem at its root using a variety of solutions with the carriers to try to limit the calls. That, as I've described, is the first course of action.

The second course of action—and you're right—is especially important for more vulnerable populations, new Canadians who may be less familiar with the system and authorities, elderly people and so on. We use educational tools. We work carefully with other departments. You mentioned the CRA, so during tax season we work with them to put out messages. We also have an intelligence branch that collects information, so we spot the latest trends and patterns and we share that information with law enforcement. We share that with the public through tweets and other means.

If I could go quickly to the last one, I'd have to take an undertaking with respect to numbers. We don't track it in that way. We don't keep numbers on how much we spend on intelligence gathering versus on getting customer complaints. Obviously we could provide you with statistics from the commission for Steven's group and his part of our budget, but we'd give you only macro numbers.

Mr. Han Dong: Thank you, Ian.

The reason I'm asking this is that I think the public wants to know—they want a number—how much government agencies are spending to fight these scams and, on the accountability aspect, whether or not we're yielding the result that we're aiming for. If we don't have a target or we don't have a goal, it's really difficult to achieve anything.

You talked about working with the RCMP. For last year, do you know how many convictions came out of these investigations? When people report fraud and it's being investigated, what happens next? What's the process? How many convictions are there?

Then we can talk about whether or not there needs to be an amendment to the Criminal Code and whatnot. I don't even know how many convictions there have been. I haven't seen any on the news.

● (1555)

Mr. Ian Scott: No, to be clear, we don't have that information. You would have to ask law enforcement agencies or perhaps the justice department. That isn't our role. We're not doing that. Where we suspect, for example, criminal fraud, we share that information and provide it to law enforcement agencies so that they can pursue it. As to how many of those investigations bear fruit or how many convictions there are, you'd have to raise that with the RCMP or other law enforcement bodies.

Mr. Han Dong: Okay. I want to get your advice. What can we, as parliamentarians, do in terms of amending laws, making them tougher, broader and more up to date to fight this phenomenon? All the good things I'm hearing about and the progress I'm hearing about are not changing the direction of these criminal activities happening. Where should we spend more energy or more resources? Is it on law enforcement?

Mr. Ian Scott: That's a fair question. I'm going to ask my colleagues to add.

I'll give you two things. I'm a good bureaucrat, and I'd never say no to more money, and I'm sure Steven and Alain would like to have—

Mr. Han Dong: If money could solve this problem, then....

Mr. Ian Scott: —more colleagues, so if you'd like to send some more money to the CRTC, we will use it properly. I can assure you of that. But simply adding more people doesn't solve the problem. First we can focus on education and compliance. We try to get people to abide by the rules. We educate them. As I said, when we get information about fraudulent activities, when we discover those kinds of actions, we pass that on to law enforcement.

One thing I would say that definitely would assist us would be having more flexibility or an enhanced ability to share information with other players, other government departments and agencies, and perhaps international partners. We're very restricted in information-sharing.

Mr. Han Dong: Could you name a few? I think I'm out of time.

Mr. Ian Scott: Could I ask for indulgence, perhaps, since we have a bit more time, Chairman, just to give one or two examples?

The Chair: It's Thursday afternoon, go ahead.

Mr. Ian Scott: Mr. Harroun, what do you want—more money? Yes, forget that one.

Mr. Steven Harroun: It's always more money.

I think our challenge is that we share a lot of aggregate information with law enforcement partners—municipal, provincial and federal. For us to say, okay, here's a campaign with very specific details, we are unable to do that on any of those levels. I'm not sure what piece of legislation it is, but sharing that information to very specifically go after this person or this thing is something we're unable to do right now under our legislation.

The Chair: Thank you very much.

We'll now—

[*Translation*]

Mr. Alain Garneau (Director, Telecommunications Enforcement, Compliance and Enforcement Sector, Canadian Radio-television and Telecommunications Commission): Pardon me for interrupting, Mr. Chair.

[*English*]

I would just add a few points on what Ian mentioned.

On how much we spend on this, the only thing I can say for sure is that when we set up the DNCL, the do not call list, we also created the do not call list operator. The role of the operator is to, of course, receive and compile complaints and to share the complaints with us, but also to collect the portion of the fee that the CRTC needs to execute its mandate. If I have to put an amount on it—it's in the DNCL report—it's $3.3 million. Is it enough? That's another question.

Mr. Ian Scott: That's the cost of running that particular program.

Mr. Alain Garneau: I echo Ian's and Steven's comments—it's a global problem. We need collaboration. We need co-operation. We don't have the tools in our hands to sit at the same table as the RCMP or the other law enforcement agencies. You must understand that the regime is a civil regime actually. We're not police officers. I don't have guns. Steven doesn't have guns.

Sometimes the modus operandi is a mix of extortion and.... At some point it becomes very difficult for us to sit at the same table and openly share information with law enforcement agencies.

● (1600)

[*Translation*]

The Chair: Thank you very much.

I now turn the floor over to Mr. Lemire for six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Mr. Chair, I'll obviously be the last one to criticize you for allowing time.

I'm going to repeat the same joke I made the last time we studied this issue. We Quebec francophones have an advantage: when we get a call in English, we know it's probably fraud.

In its 2020 report, the committee said it hoped there could be greater cooperation among government agencies, including the CRTC, the RCMP, the Competition Bureau and Innovation, Science and Economic Development Canada. The committee had heard lengthy testimony and many solutions. It was also determined that consumer intervention was needed to detect fraud.

On November 30, 2021, the CRTC issued a news release announcing a new technology called STIR/SHAKEN, which was intended for telecommunications service providers and enables them to detect calls made from phony numbers.

From what I understand, only one company, Bell Canada, responded to your announcement. What about other telecommunications service providers. Are they making an effort too? Where are they?

Can you cite any examples of initiatives designed to combat efforts to defraud the clients of those businesses?

Mr. Ian Scott: This involves all the major providers and many smaller businesses.

Mr. Garneau, would you like to answer the question?

Mr. Alain Garneau: With pleasure.

The Bell case, which is recent, was mentioned. I think it's a very good example of a business that takes matters into its own hands. Rogers recently made a real breakthrough too. It adopted an artificial intelligence-based technology that uses algorithms to provide call recipients with caller IDs or at least to let them decide whether calls seems legitimate.

You have to understand that the purpose of the STIR/SHAKEN technology isn't to block calls but rather to provide people receiving them with the information they need to decide whether they want to pick up once the calls have been validated at level A, B or C. Without going into the details, the role of the service provider through which the call is made will essentially be to authenticate the call by certifying that it comes from one of its clients, that it knows the individual and that it is indeed Ian Scott, for example. The service providers of individuals who receive calls will confirm that they may answer it and that it is indeed Ian Scott who's calling, not someone in Europe who's trying to defraud them.

Mr. Sébastien Lemire: We observed during our 2020 study that small service providers found it hard to implement these solutions, which—correct me if I'm wrong—work well on smart phones but less so on home landlines.

The elderly are the most vulnerable. They have a landline at home and probably receive most of these calls. Are there any solutions out there to address these residential call cases?

Mr. Alain Garneau: Allow me go back a little in time to provide you with some details.

Our first step was to address calls made using VOIP technology, the Internet protocol. The reason for that is simple: TDM networks, which use time division multiplexing, are still in widespread use in Canada. Requiring providers to migrate to VOIP technology is one thing, but you have to understand that costs are associated with that. So you have to proceed gradually. That'll be the next step.

The United States has adopted or mandated out-of-band authentication, which makes it possible to certify calls even if they're carried on a TDM network. That's the approach we adopted in Canada. You have to understand that the Canadian market is smaller than the American one. You also have to consider the access to technological solutions that vendors provide.

For smaller service providers, the CRTC recently requested that the Canadian Secure Token Governance Authority increase their coverage so those providers could have easier access to those tokens too. So we're doing something for the small players.

The resellers among them can participate through their service provider, which will be able to validate their calls.

● (1605)

Mr. Sébastien Lemire: So I understand you're satisfied with the efforts the industry has made.

Are you also satisfied with the way government agencies are cooperating at this stage? Can steps be taken to reinforce this agreement even further, or is that a problem?

Mr. Ian Scott: Generally speaking, everyone's cooperating.

As Mr. Garneau said, however, sharing information is a problem because the act lays down limits in that regard.

Mr. Sébastien Lemire: Then let's hope that it can be done and that it can be promoted further.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Lemire.

Mr. Masse, you have the floor for six minutes.

[*English*]

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

Thank you to the witnesses for being here today.

Maybe my first intervention could be to ask our analysts to look at the 15 recommendations that were in the previous report and whether they were acted upon, and to put those in as part of a package to ourselves. There are 15 in total.

I will go to Mr. Scott.

Recommendation 5 was about legislation for information sharing between you and the RCMP.

Was there ever any reaching out by a government department or minister or any bridging to deal with that? That was based on your testimony from last session where we were looking at sharing that information because it is, as you noted, a big issue and jurisdiction is still there.

Mr. Ian Scott: Thank you for the question.

I'll ask Mr. Harroun to add, but I'd just start by saying that we have an ongoing discussion with those partners, but, as you would well know, opportunities to change or revise legislation don't arise often. We have yet to have an opportunity to have a fundamental review of the legislative provisions, but the need has been communicated and recognized. Obviously, I don't speak for the minister, and the ministry responds to the recommendations of the committee, but I would say that we certainly feel that we have been heard and that they are aware of the challenge.

Steven, you deal with the department on a more regular basis. Do you have anything to add?

Mr. Steven Harroun: No. There's nothing official, as Mr. Scott has indicated, but we continue to work with our law enforcement partners to the best of our ability. We would welcome that change. We welcome that recommendation.

Mr. Brian Masse: It's one of the things we can control in all of this.

I don't like the characterization of this issue as nuisance calling. I've had constituents who have committed suicide after falling prey to this—after losing financial means through this, with the shame and so forth. It's pretty serious.

I'm just wondering, with regard to the communication element again, how strong you are in terms of what we could advance as next steps on this. I really applaud your efforts to move what you have forward. If we can actually get that, maybe we can instigate to get the Privacy Commissioner to intervene to make sure there are proper guidelines and confidence. I see that as low-hanging fruit for us to take advantage of. It's nothing that costs us money, but it's something we can control.

Mr. Ian Scott: Let me take a step back. If I use the term “nuisance calling”, first of all I'm referring to certain kinds of calls. These are grave issues. There is no doubt about that. I generally refer to these as “unwanted communications”. We have other challenges about getting broadband to everyone and wireless to everyone. In this case, we want to stop unwanted communications and protect consumers. That's what we're endeavouring to do, and we will work with anyone in that regard.

I don't know whether engaging the Privacy Commissioner, for example, is going to—

If I can just finish—

● (1610)

Mr. Brian Masse: If I can intervene, my time is short.

Here's what I'm trying to get. I'll segue with this: You mentioned resources. If we're going to get some bang for our buck, so to speak, what are we looking at if, for example, we put a million dollars into the CRTC specifically related to fraud or whatever. I don't know what it is. Can you come up with a plan so that we, as legislators, can look at that and then see what potential results we can get? You have made some good progress. What I'm looking for is easy steps we can take right away to deal with this. That's kind of where I'm trying to go, Mr. Scott.

Mr. Ian Scott: I understand.

With respect, if there were easy steps to take, we'd take them. We're not poor, and we've applied the resources we have effectively. As technology evolves, people with bad intentions and criminal intentions use technology to subvert the system. All of us can use more funding and apply more horsepower, but the measures we're taking are all effective and we would simply do more of what we're doing. If we recognized that something was obvious and would have an immediate impact, honestly we would be working in that direction, and we do. We're reaching out all the time with our partners to try to expand and do what we do better.

Mr. Brian Masse: Do you have a number in terms of how much in administrative monetary penalties has been added over the last couple of years since the study was done? Is there a number the committee can get on that? What I'm looking for is that often we see that a lot of preventative measures can be taken that will affect our economy in a very positive way, as well as disrupting this. I'm just wondering what our cost benefit for this is. Do you have a number that could be shared?

Mr. Ian Scott: Steven can give you a general number, and we'll follow up with specifics if you'd like.

I'd just like to preface this by saying that our first order of business is prevention, education and compliance seeking. We use enforcement for what it should be—a secondary measure. When we're talking about do not call and so on, that is the way we approach enforcement.

Steven, can you give a ballpark at this point?

Mr. Steven Harroun: It's in our annual do not call list report. To date, we're at about $11 million over the last 10 years. In the past year it's been about $600,000.

I think the point to make here, and what Ian was alluding to, is these are the administrative monetary penalties that companies have willingly...or have been charged with because they have violated the telemarketing rules. These are legitimate players who are, if you will, paying for the sins of the past and, “Oh, we didn't buy the list. We didn't call the right people at the right time,” etc.

I think what you're speaking to, Mr. Masse, is more the fraud-related side of this piece, the 50% that is fraud. That's not where we can apply our administrative monetary penalties.

If I could just go back to your previous question, Mr. Masse, I think what's important to understand is that we are a civil regime. You could give me $10 million tomorrow and I'd be very happy, because I could have the entire CRTC working on telemarketing cases and anti-spam cases. However, we are a civil regime, not a criminal regime, so it still might not have the impact you want on the fraud side.

Mr. Brian Masse: I understand that, so I'm going to interrupt right here.

What I want is a proper business plan. The CRTC represents the public, and you're coming here. I can invent numbers, too. I'm sorry, but I'm a little upset with this. Present us a business plan in terms of what you can do and how effective it can be. I don't know exactly whether it's $10 million or $2 million or $1 million. This is pretty serious and a priority to me, as a member of Parliament, and I think to a lot of members of Parliament. Put a plan together and show us exactly what it is. That's what you're supposed to be doing.

I know my time's up, but at the same time, I'd like—

Mr. Ian Scott: With respect, Mr. Masse, we file a report with Parliament—

Mr. Brian Masse: Okay, but you're at committee here—

Mr. Ian Scott: —and it has all of that information.

Mr. Brian Masse: You're at committee here and you're throwing out that you need more resources, and then there's $10 million and there are other...and all I'm asking for is a simple plan. Seriously, are you going to fall back on the idea that I'm supposed to read that report or have that at my fingertips right now?

Mr. Ian Scott: I didn't ask for more money. I was answering a question with respect to what would help.

As Mr. Harroun just said, we can give you those numbers, and those numbers are contained in our report to Parliament. I think there is good value for money with respect to the telemarketing regime. Alain told you that with respect to telemarketers, it's on a cost-recovery basis.

As to the criminal side of this, or, if you will, the elements that are engaging in criminal activity, obviously there are no numbers. How would you possibly estimate that?

● (1615)

The Chair: We'll have the opportunity to get back to this, Mr. Masse, if you want, but in another round of questions, because we're way over time again.

I'll now move to Mr. Deltell for five minutes.

[*Translation*]

Mr. Gérard Deltell (Louis-Saint-Laurent, CPC): Thank you very much, Mr. Chair.

It's always a pleasure to be here, colleagues. I remember a good old saying that I used when I was a journalist: "When it's good, it's never long." I thought Mr. Masse's questions were very good and relevant.

Generally speaking, you always get the best and the worst with these calls. That's also true of virtually all information technologies. You can have excellent tools and then see them used in unacceptable ways.

And let's not fool ourselves: we're all politicians here; we all ran election campaigns a year ago, and I bet we all used robocalls. I'm very proud of my white hair, which proves I'm not the most adept person in this area, but in the end I agreed to spend a little money on robocalls, which is quite unusual for me. I have to admit I was really impressed with the real results I got; the calls let me contact 2,000, 3,000 or 4,000 persons an hour. I have to say it's cost-efficient.

You mentioned the initiative that Bell Canada took in response to your invitation to detect and address fraud proactively. That's the kind of initiative we should promote and encourage. When private businesses that thrive on these calls decide to discipline themselves that way, we acquire better tools for the future. So I welcome that great initiative.

Now I want to discuss more technical matters in all this chaos.

First, is there any way to block at source calls from outside the country, whether from the United States or another unknown and distant country? Is that technically and legally feasible? Obviously, everything can be done under an act, if necessary. Could Canadian telephones be configured to block all numbers from area codes other than 418 or 613, for example?

Mr. Ian Scott: Would you please answer that, Mr. Garneau?

Mr. Alain Garneau: Yes, that's a technically feasible option. Under the STIR/SHAKEN model that the French have adopted, starting in 2025, France will be required to block all international calls that haven't been validated. But that approach wouldn't promote good relations with our neighbour to the south.

However, the technical means do exist. Without responding once again to questions that have already been asked, I'd definitely invest in that area if I had other resources at my disposal. We'd have to see what can be done across networks to roll out systems that can detect those calls in order to control them more effectively. That would allay a lot of fears.

Mr. Gérard Deltell: Thank you, Mr. Garneau.

I see Mr. Scott seems open to the suggestion. Is that a position the CRTC could adopt, or is it only a thought that you just stated, Mr. Garneau?

Mr. Alain Garneau: No, it's definitely nothing the CRTC has considered.

I just want to say that we've adopted a three-part approach.

First, as Mr. Harroun mentioned earlier, there's a limit to what we can do to implement a solution. If we had more money, we could process more files, but, ultimately, there'd just be more people addressing the issue.

Second, we work hard to increase awareness among small businesses, but also among seniors, a little surprise that I'll let you discover in our next report.

The third pillar is all the upstream work we're doing, which Mr. Scott discussed.

[*English*]

Bell blocking, universal call blocking, STIR/SHAKEN, call traceback.

[*Translation*]

All that's being done upstream, and a lot of work remains to be done in that area.

● (1620)

Mr. Gérard Deltell: Would it be possible to give telephone service customers an option to block all robocalls systematically? Could something like that be done? Is it done in other countries? Have any companies previously assessed the option? What are your thoughts on the subject?

[*English*]

Mr. Ian Scott: You have to know they're robocalls.

[*Translation*]

Technically, we don't know. The purpose of the STIR/SHAKEN technology is provide a measure that increases consumer confidence.

[*English*]

Mr. Gérard Deltell: Do you know if that's applied somewhere in the world? Is there a situation in the world that has an opting out, so that, if you don't want to have any robocalls, you can add the application and then that's it; that's all, folks; it's over?

Mr. Ian Scott: Yes, the French model will look something like that in the future.

The balancing act here is to try to block unwanted or illegitimate calls but not to block legitimate ones. That's the challenge. You can say, yes, we'll block everything that we're suspicious about, but that means we'll be blocking legitimate calls, and consumers do not want that. Consumers want illegitimate calls blocked. We're trying to equip them with the tools to give them trust in the system.

[*Translation*]

Mr. Gérard Deltell: That's why a lot of people, including me, don't want to pick up when they don't know who's calling. I have voicemail for that.

Mr. Ian Scott: [*Inaudible*] of mobile calls are fraudulent.

Mr. Gérard Deltell: Right.

With fraudulent calls, do you see a difference between people who have cell phones—the vast majority—and those who still have landlines, or do fraudsters strike the same way everywhere?

Mr. Ian Scott: No, not really.

Mr. Gérard Deltell: Is there a difference?

No, there's no significant difference.

Mr. Gérard Deltell: How can we distinguish welcome calls from unwelcome ones? Many people think it would be simpler if they had the option of blocking all unwelcome calls.

[*English*]

Mr. Ian Scott: If Alain can answer that, I'm going to give him a promotion.

Mr. Alain Garneau: Okay, here's my answer.

Mr. Ian Scott: Sorry, if he can do that.... Let me rephrase it.

Mr. Alain Garneau: Too late.

[*Translation*]

That's a very good question. I obviously can't disclose certain information that we obtained in the Bell Canada case, but I can tell you that telephone service providers obviously monitor their networks and can detect anomalies. For example, if 12,000 calls a minute are made to area code 514, something abnormal's probably happening. That's a major indicator.

Mr. Gérard Deltell: But, as is the case in an election, everyone can call that number or at least try. Everyone's making thousands of calls simultaneously.

Mr. Alain Garneau: I'm talking about a single number, from any country, that would generate 12,000 calls on the network.

[*English*]

Mr. Ian Scott: If there were thousands of people with the same number voting, it would be a problem too.

[*Translation*]

Mr. Alain Garneau: The Telecommunications Act does not give telephone service providers the right to introduce these mechanisms themselves. They have to ask permission from the CRTC, as Bell did.

The Chair: Thank you very much.

Ms. Lapointe has the floor now, for five minutes.

Ms. Viviane Lapointe (Sudbury, Lib.): Thank you, Mr. Chair.

[*English*]

Mr. Scott, earlier you talked about the first intervention being prevention and education. I'd like to know what kind of work the CRTC does with its partners to raise awareness about fraud calls.

Mr. Ian Scott: Sure, and I'll ask Steven to elaborate. He runs this group.

The obvious things are communications with the public and working in partnerships with various players. I'll quickly outline them.

One, we have an intelligence-gathering group that examines everything that goes through the fraud reporting centre and all the information we gather to identify emerging campaigns. One of the members mentioned earlier how the day after the government announces a program, you get fraudulent calls in relation to that program.

During tax season, we work closely with Canada Revenue Agency to remind people that the Government of Canada doesn't threaten you by text message or over the phone with jail sentences or what have you.

In an ongoing education campaign, we speak at universities, fraud conferences, at commercial conferences where telemarketers gather, and so on.

Steven, rather than my bouncing around here, do you want to give, perhaps, a better response?

● (1625)

Mr. Steven Harroun: No problem.

I think what's important is that we do engage various levels, including Joe and Jane Canadian. We try to get that message out through some of our government partners, but we also talk to industry associations. I speak a lot at various conferences, as Ian said, but we also work with our colleagues at the Competition Bureau and the Office of the Privacy Commissioner, and when we see information, we share it with each other and help support campaigns.

October—I was going to say it's next week—is anti-fraud month, so we'll be participating with the CRA and the Competition Bureau and others who will be putting out messages on a regular basis. We have an amazing communications team at the CRTC, which gets messages out via our website, our social media channels, etc.

We try to be as active as we can in the space.

Ms. Viviane Lapointe: I appreciate that. I'm thinking specifically about seniors. Those are the calls I get most in my constituency, from seniors who may not be on computers or have smart phones.

How are you able to share or disseminate information to the vulnerable population of seniors?

Mr. Ian Scott: I'm not sure we have an easy answer for that or a simple method to reach them. I can use my own example. Perhaps you're in a similar circumstance. My sister and I give our elderly mother a lot of advice about what to answer and what not to answer, and we ask her to check with us on things. If you will, you educate those to educate others.

You're right. For those who are perhaps new Canadians with less familiarity with French and English and for some elderly populations, we need to go through intermediaries. We reach out as broadly as we can, but I won't pretend that we can reach everyone.

Ms. Viviane Lapointe: Are there particular types of calls that Canadians tend to fall victim to more than others? Do we know that?

Mr. Ian Scott: I'll say—and Alain may want to add—that I think it's a bit facile to say this, and I apologize for that, but it's the cleverest ones. Particularly if we're talking about fraud, they're very opportunistic. When the government introduced an income support program in the midst of COVID, it took them a matter of hours to put out messages saying, “This is where your name is on the list” and “Call this number or text here in order to get your rebate” or whatever.

Immediately after the Rogers outage, they were sending out “Rogers owes you money. Text here or call here to get your refund.” They're very quick. Some of them are very sophisticated. Even within government we have it. I've had employees who have received emails from me, apparently, and they've been clever enough to know I don't usually ask people to go out and buy thousands of dollars of iTunes cards. We do get questions, as do municipalities, about needing to wire money to cover a contract or whatever.

There are large-scale ones and small-scale ones, but they're clever, and they are very quick to take advantage of public announcements and so on. I think those ones are probably the most effective.

Alain, do we keep specific statistics that you're aware of, as far as you know?

Mr. Alain Garneau: We have some. As Steven mentioned, we have an intelligence shop, the role of which is to gather all the information, so I wouldn't be surprised if we had some. I don't have those statistics with me at the moment, but definitely I have no worries that—

Mr. Ian Scott: I will undertake to have our staff look at it, and if we can provide a better response, we will send it to the committee clerk if that's okay.

Ms. Viviane Lapointe: I appreciate that.

I just want to touch upon MP Masse's point about how the number of individuals who actually report scams is quite low. I would be interested in knowing what you think is the reason for that. Also, would an increase in reporting help the CRTC and its partners address those challenges that we currently face with fraud calls?

● (1630)

Mr. Ian Scott: On the second point, yes. The more information we have, the more specifics we have about the nature of campaigns and the nature of the calls, the better armed and prepared we are to educate consumers, to put law enforcement or other parts of government and the public on notice, so absolutely the more information the better.

On the first part of the question—

Steven, sorry. Go ahead.

Mr. Steven Harroun: On the first part of your question, on the telemarketing side we receive about 3,000 complaints a month. On the spam side—that's your SMS texts or emails—we get about 5,000 a week. We are not shy on complaints.

You're right. Canadians consistently under-report. They are either embarrassed if they have fallen for a scheme, or they just don't want to go through the motions of reporting it. My intelligence teams use those complaints. That's why we talk to service providers. That's why we talk to the banks. That's why we talk to other areas that have information on what Canadians are complaining about so we can slice and dice that and see where the common threads are and see where the common campaigns are and see if there's something we can do about it or if one of our partners can do something about it.

[*Translation*]

The Chair: Thank you very much.

It's over to Mr. Lemire now for five minutes.

Mr. Sébastien Lemire: Thank you, Mr. Chair.

I'd like to ask the witnesses once again about the matter of smaller providers. Can they really respond as quickly as you require? Can they invest as rapidly as the major service providers? Do you believe that their capacity for protecting their customers can compare with the major providers?

Mr. Ian Scott: I think so.

Mr. Garneau, would you like to answer that question?

Mr. Alain Garneau: The answer is yes. Most of the new smaller providers are already using the IP network. It is therefore not an additional burden for them. Those that are not can rely on their upstream provider to handle this aspect on their behalf.

We have not yet received any complaints. To my knowledge, no provider has told us that this new requirement is too much of a burden.

The only hitch reported does not come from the industry side. For the STIR/SHAKEN technology to work, certain technical capacities are required, including software and switching equipment. There also has to be an IP interconnection agreement. It's with things like this that the smaller providers might sometimes have to wait longer, which is only to be expected. Agreements with the major providers like Bell Canada or Telus are generally in place earlier than for the smaller providers.

Mr. Sébastien Lemire: Further to the Rogers outage this summer, the Minister, Mr. Champagne, required more collaboration among telecommunication service providers, because this outage had revealed the limitations of our system.

Could collaboration of this kind be used to address fraud issues? How could the other providers come to the assistance of those that had shortcomings?

Mr. Ian Scott: That's not exactly the same situation, nor does it have the same goal.

[*English*]

Reliability measures are to protect against outages. The focus is not there on sharing information of this type, but there is co-operation within the industry to combat this.

[*Translation*]

Does that answer your question?

Mr. Sébastien Lemire: Yes, for now.

I understand that there is still some work to be done, but overall, is there a concrete action plan in the works to modernize the networks?

To increase the level of security, there are also robustness and resilience considerations, as you mentioned. Is that where we are headed now?

[*English*]

Mr. Ian Scott: With respect to whether we're really focusing on the issue of the robustness and integrity of networks, that really falls first and foremost to the industry department, to ISED. They work with the industry. They deal with natural disasters, with emergencies. They operate CSTAC, that committee, so it really is they who are responsible for that. Our role as the regulator of their business...that's not so much our role.

With respect to telemarketing, it's the other way around. It's very much us, and us working with the carriers, but I would say on both fronts that there are both plans and co-operation between industry participants.

● (1635)

[*Translation*]

Mr. Sébastien Lemire: One of the recommendations made by the committee two years ago was for the Government of Canada to launch a month-long awareness campaign in local and national media to help protect Canadians against fraud, particularly forms of fraud related to COVID-19. Do you know whether this recommendation was implemented and what steps were taken to make the public less vulnerable to attacks?

Mr. Alain Garneau: Every year, the CRTC works with the Competition Bureau and the Canada Revenue Agency on the Fraud Prevention Month campaign. Scams were identified early on in the pandemic and we played an active role in delivering messages to Canadians. In short, yes, there were meetings and communications with the Canada Revenue Agency and other organizations to coordinate efforts.

Mr. Sébastien Lemire: Thank you. That's good news.

The Chair: Thank you, Mr. Lemire and congratulations once again on your ability to keep to your speaking time better than anyone else around this table. I'm grateful to you for simplifying my work.

Mr. Masse, you have the floor for five minutes.

[*English*]

Mr. Brian Masse: Thank you, Mr. Chair, and thanks for the heads-up warning.

Mr. Ian Scott: I thought it was directed at me, Mr. Masse, not you.

Mr. Brian Masse: It's all good.

You mentioned collaboration about the industry. Is there a formal working group in the industry? What CEOs or staff have they assigned? Are you part of those discussions? Give us a little more detail as to what's going on in the industry.

Mr. Ian Scott: Let me ask Mr. Harroun to respond to that. He's more in touch with it on a day-to-day basis.

Mr. Steven Harroun: Absolutely, and thanks for the question.

All the major providers, and even some of the smaller providers, participate in a couple of different working groups at the staff level so that we have the right technical folks on board and the right regulatory folks on board. When necessary, it is more of a technical group. We look at the intelligence they're seeing with respect to their networks, at what kind of traffic they're seeing, etc. They meet on a weekly basis.

On a monthly and quarterly basis, we have a larger group, which we call the VOIP telephony group, which talks about all the issues within that area.

Mr. Brian Masse: Would it be helpful at this point in time to heighten or increase the responsibility on the carriers to also make this more public at a more senior level as well if there is going to be some more awareness? If it's a bunch of IT people meeting or on Zoom, it's one thing, and it gets real results, but also, is there something more we can do on the culture of this with regard to the telcos?

Mr. Steven Harroun: The telcos are definitely very actively engaged with us at the more senior levels. Obviously, that's at your discretion to make that more public and ask them to inform their consumers more.

I will say, as I've mentioned before, that of all the different partnerships we have, the telcos, the banks and others are very active in the space in informing their customers when there's a fraud. They all have blinking lights on their websites: “This is the latest scam.” Unfortunately, that changes on probably a weekly basis. They all are very public facing. Could they do more? Could we all do more? Absolutely.

Mr. Brian Masse: Okay. The reason I asked about the fines and the penalties is that, at the end of the day, a fraud call, whether it's done by a carrier that is stretching the rules or whether it's an outright organized crime thing, it's still the same result for the victim. On the penalties you mentioned in your testimony, this is what I'm trying to get at.

For the $10 million you mentioned—that was your number—I'd like to know, what does that buy for the public in terms of an improved crackdown or stopping fraud calls? What type of an investment and return do we get on that? That's what I'm really seeking with regard to even having this come back to Parliament here. It's how far we've come, but also where we can go. You mentioned $10 million. What does that actually gain for our economy, our consumers and public protection?

● (1640)

Mr. Ian Scott: I'm trying to think of the specific reference. I'm not being disagreeable, Mr. Masse, but I think Steven mentioned that even if he had $10 million, it would be.... That wasn't the point of that.

I think there are different issues here. Telemarketing—

Mr. Brian Masse: That's fair. I'm sorry but I'm just going to interrupt because I have a short amount of time.

This will be my final thing. All I'm looking for is that, hopefully, you can come back to us and give us a picture as to what, if we had some improvements, those would cost the CRTC, and if we invested in those, what our return might be. You don't have to come up with it now, but that's what I'm looking for. If we help with these things—just as with the communication piece and how you still don't get the proper communication because of sharing of information laws—I'm looking to see where we get value out of that. If you are missing some things later on, we'd love to hear that. That's what I'm looking for. How do we exercise that? How do we give you the proper supports to get the results? Could you to do that?

Mr. Ian Scott: That's a very fair request. We'll consider that. Thank you.

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

Thank you to the witnesses.

[*Translation*]

The Chair: Thank you, Mr. Masse.

You can go ahead now Mr. Généreux, for five minutes.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

The Canadian Anti-Fraud Centre has reported that it has received over 50,000 fraud reports since the beginning of the year, amounting to estimated losses of $285 million.

But Statistics Canada believes that fraud is consistently underestimated because only 13% of offences are reported to the police.

I don't know how Statistics Canada determines that only 13% of fraud is reported, but if this percentage is accurate and represents 50,000 fraud reports and $285 million, then we're potentially talking about $1 billion extorted by fraud. Are my calculations correct? Is my estimate right?

Mr. Ian Scott: Yes.

I'll let Mr. Garneau answer.

Mr. Alain Garneau: Your estimate is accurate, if the rule of three is anything to go by.

As we said, it's not our role to obtain this information, but the figures match what we have been hearing from other law enforcement agencies. Generally speaking, only about 10% to 15% of victims complain.

As Mr. Harroun said, there are several reasons. The victims may be embarrassed or feel remorse, or perhaps have the impression that they'll never see that money again. That's why so many people don't complain. They decide to live with what happened to them, treat it as a lesson learned, and move on.

Mr. Bernard Généreux: You're talking about people who are victims of fraud, not just attempted fraud. Am I correct in saying that the monetary estimate of all this fraudulent activity amounts to much more than has been reported?

We're talking about telephone fraud. Today, on the smart phones that we've had for 25 years now, we regularly get lots of text messages, which wasn't possible on landline phones.

On the basis of these numbers, are you seeing an increase in fraud attempts? You must have seen an acceleration or increase in such attempts, not only in te form of telemarketing by telephone, but also, I would imagine, via text messages. Do you deal with that as well?

Mr. Alain Garneau: As Mr. Scott mentioned, Canada's anti-spam legislation governs everything to do with spam, email and text messages. The CRTC also deals with it, but with a different team than mine.

To answer your question, it always amounts to the same thing. Whether the fraud attempt is by means of a telephone call or in a written text message, the goal is the same, which is to obtain someone's personal information to sell it, or to use it to defraud someone or make money from it.

Mr. Bernard Généreux: Since the start of our meeting, the Canada Revenue Agency has been mentioned of number of times, including by two of my colleagues, Mr. Dong and Ms. Lapointe.

According to you, are fraudsters most frequently pretending to be from the Agency?

● (1645)

Mr. Alain Garneau: There are trends. For example, at income tax time, there is likely to be a significant increase in fraud attempts that use the Canada Revenue Agency as a cover. However, other agencies were also frequently used, such as Border Services Canada for imaginary Amazon parcels held at the border. There are all kinds of scams.

Before coming to this meeting, Mr. Scott spoke about what is called the "Mandarin scam". These were fraudulent calls that were originally only in Mandarin. Most people who answered and heard someone at the other end of the line speaking in Mandarin would usually simply hang up because it wasn't their language. The scam was clearly focused on people whose culture or language was from Asia. But Mr. Scott told us that he had received one of these calls recently, but that on this occasion he had been given the option of hearing the message in English or in Mandarin. So things have been evolving.

Mr. Bernard Généreux: Mr. Harroun, since the start of the meeting, you have been referring to information and education. You said that you give talks and provide lot of education.

I'm from a remote region rather than from downtown in a Canadian city. What methods do you use to make specialists in this subject more aware? I've never seen you in La Pocatière or Rivière-du-Loup, for example. Do you make use of local or regional media.? What tools do you use to provide this type of education?

I've already seen some ads, but I can no longer remember whether they were from the CRTC. I believe that the Canada Revenue Agency had its own ads on matters like fraud.

Mr. Ian Scott: We are all involved. As you were saying, the Canada Revenue Agency makes its own ads. We post messages on our website, and Mr. Harroun works with entrepreneurs and businesses from everywhere. So I believe our messages are disseminated evenly across Canada.

Mr. Bernard Généreux: I don't wish to offend you, Mr. Scott, but I rarely go to your website. The general population needs to be informed on more traditional media, especially elderly people, as Ms. Lapointe mentioned earlier.

I get calls from people in my riding who still have a landline at home and use neither the Internet nor a smart phone. These people need to be informed via traditional media. Is that something you still do?

Mr. Ian Scott: Yes.

Mr. Garneau, Would you like to add anything?

Mr. Alain Garneau: I'd like to go back to Mr. Harroun's explanation.

For us to consider something to qualify as telemarketing, the call has to have a business purpose. Whether the company is legitimate or not, it must offer a product or service. If the call is criminal in nature, it amounts to saying that the person is using the telecommunications network to commit a crime, which is not a part of the CRTC's mandate.

By analogy, it would amount to saying that if a person was driving a Dodge van while committing an armed robbery, the automobile dealer would be asked to do something about it. Do you get what I'm saying? When a crime is committed, even if the medium used is the telecommunications network, our mandate does not go beyond the civil level.

Mr. Bernard Généreux: What you're telling me Is that you don't consider yourselves to be responsible for telling the general population, and elderly people in particular, that there may be fraudulent activity by telephone or via text messages. Do you see what I'm saying?

Part of the population is still at risk, and I'm curious to know what percentage of the complaints to the police are by people 55 years and over. I am pretty well convinced that it's a very large number. It's a category of the population that is probably at much higher risk than young people, who are more savvy and in a better position to determine whether a call is fraudulent or not. I get calls like these just like everyone else, even if they're not in Mandarin, and I can tell the difference.

What I want to know is whether you use a special approach or particular terminology to reach these people.

● (1650)

Mr. Steven Harroun: I understand what you're aiming at, and it's what I want too.

On an airplane recently, I was speaking with an elderly woman, and I asked her if whether it might be helpful to have students discuss these things with older people, or whether some other approach of this kind could be used for people who go to a community centre and who speak neither French nor English. The goal here is prevention, and in the end, I would like all Canadians to benefit.

[*English*]

If I can prevent Canadians from falling victim to these things, I've done my job. It's not about an AMP. It's not about compliance. At the end of the day, it's about education if you have not fallen victim.

Mr. Ian Scott: Perhaps I can very briefly add something, Mr. Chairman.

Your point is well taken, and I think we can do better. We do things on public radio and so on, but you're right, and I'm taking note that using conventional media and using other vehicles to get those same messages out is a desirable thing. We can and should do better.

[*Translation*]

The Chair: Thank you very much, Mr. Généreux. I like the way you reminded us that elderly people were more vulnerable, but that savvy young people know how to recognize scams and don't answer, just as you don't. I've always thought of you as a savvy young person Mr. Généreux.

Mr. Gaheer, you now have the floor for five minutes.

[*English*]

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair.

Thank you to the witnesses for making time for the committee.

I do want to underscore, for the sake of the committee, one more time how important this issue is and that it's not just nuisance calls. I know of cases from before I entered politics of seniors from ethnic backgrounds, from minority backgrounds being targeted in their native language. They were told that within an hour, they had to deposit *x* amount of money, and that otherwise they would lose their citizenship or lose their permanent resident card, and they actually did that. I know of one particular case in which the individual actually then committed suicide because of the embarrassment of the entire ordeal, so it's a very serious issue.

Mr. Scott, you spoke a little bit about the international co-operation that happens between your organization and your international counterparts. Do you want to elaborate a bit more? I feel as though we're bringing a lot of people into the country every single year and we need to take care of them and protect them because they're vulnerable. What is the co-operation that's happening?

Mr. Ian Scott: First, I want to reiterate that, as I believe you are the second member to make this point, this isn't just about nuisance, and you're absolutely right that this is very serious. The numbers the member quoted, in terms of potential amounts associated with fraud, are huge, and the societal impact is huge. That's why we are seized of this issue, so you have no disagreement from us.

What we try to do, as I said earlier, with international organizations is to share best practices, leverage our knowledge and co-operate. I'll give you a quick example. We recently signed a new memorandum of understanding with the Australian regulator, and in part that's because the frequency of these calls is now increasing in Australia. They are sometimes different in tactics, but the overall sort of patterns are similar. To the extent that we're allowed, we'll share with them information on investigative techniques, enforcement techniques and the intelligence we gather as to how to most proactively deal with it.

I'll give you a second example. The new recently named chair at the FCC and I have met twice now. One of her main areas of focus, as it was for her predecessor, is robocalls, as they tend to refer to them in the U.S. We're working together. For example, we're going to try to enhance our call tracing activities so we can identify and trace calls and say, “Okay, they're coming into Canada from the United States or from another country.” Likewise, we can work with the United States and say, “If it's coming in from the United States, where did it start?” Then we can get to the next door, so to speak. Then they are working to close those doors with their providers. So it's a combination of sharing intelligence and tactics that are working as well as identifying patterns.

The last point I'll make is that when we talk about criminal activity—and there is criminal activity in certain of these situations—then it's a question of finding the ability to pursue those matters whether in the United States or in an Asian country or wherever, because at the source, it may be in another country, and we have to get enforcement actions taken there, and that's a challenge.

● (1655)

Mr. Iqwinder Gaheer: That actually feeds into my next question. I'm going on the examples that I know of. There were centres set up in Pakistan where an entire call centre is dedicated just to making fraud calls. It's turned into a money-making operation.

In the countries you've spoken about where there is co-operation, so far I think you've mentioned America and you've mentioned Australia. Is there any co-operation that happens with South Asian countries, for example?

Mr. Ian Scott: First of all, I wouldn't point to one particular country or another. There are many countries. The majority of telemarketing generally between Canada and the United States is across borders, not from abroad. I want to be clear: We're talking about co-operating—

Mr. Iqwinder Gaheer: I'm sorry. The reason I bring it up is that my constituents are affected by that region. That's why I brought it up.

Mr. Ian Scott: I understand. I'm just always hesitant to say that there are calls coming from a particular part of the world. They come from a lot of parts. Nefarious actors can be located anywhere and use technology from anywhere, but you're quite right: There are examples there and elsewhere.

There are two different things here. We're working with like-minded agencies. Yes, we've dealt with the Indian telecoms regulator, for example. I don't know if we've had direct engagement with, for example, Pakistan's authority, but we also work within organizations such as the International Institute of Communications, which has regulators from around the world. We're hosting a meeting of them here in Ottawa in November. We raise those issues there.

There's a difference between sharing information and practices with fellow regulatory agencies and the other thing you're talking about: enforcing the law. That, we have to hand over to law enforcement agencies and the justice department to pursue and to encourage their international counterparts to pursue. That's beyond our jurisdiction and our reach, so to speak.

Mr. Iqwinder Gaheer: As a lawyer, I do understand that the executive is in charge of enforcement. From what you're saying, it seems that the CRTC lacks teeth to go after this fully, and it's law enforcement that has to come in and get the job done. I think this question was asked before as well: Is there communication back and forth? If information is passed on about a specific complaint, do you get a report back of what happened in, let's say, a month's time, six months' time or a year?

Mr. Ian Scott: The short answer to that—it's a bit unfair—would be no. As Mr. Harroun explained before—or it may have been my other colleague, pardon me—we're not a law enforcement agency in that sense. We're not enforcing criminal law. We have to hand off those things where we identify them.

Mr. Masse and I talked about this briefly. The area where we could use some legislative help, for lack of a better term, is to expand our ability to share information in both directions. That would be helpful so that we can assist law enforcement agencies in their work. I do have to draw a line. They do their work, and we do ours.

The Chair: Thank you very much.

Did you have another question?

Mr. Iqwinder Gaheer: No. Thank you so much.

The Chair: We'll move to MP Gray for five minutes.

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here.

Mr. Scott, I want to focus my questions today around an issue that was brought forward during our previous industry committee study in this area: the SIM swapping and phone porting scam. Since that study took place, what actions has the CRTC taken to prevent either of these types of fraud from taking place?

Mr. Ian Scott: Thank you for the question.

I didn't bring statistics with me today, but the short answer is that the industry has taken numerous steps, and the results have been very encouraging. The numbers of SIM-swapping activities have drastically declined.

I don't know, Steven, if you have the numbers top of mind.

A lot of the industry's work was done co-operatively under the banner of the Canadian Wireless Telecommunications Association. They said that they would introduce measures through their members to add additional layers of protection. They've agreed to various measures, and they co-operate, and those measures have resulted in a significant reduction. It hasn't eliminated the problem—there are always opportunistic actors—but it has vastly improved.

I didn't bring those statistics with me, but I can confirm that the problem is significantly lessened. I'll use that word.

● (1700)

Mrs. Tracy Gray: That's great. Thank you very much.

As you said, if you have that information and would be able to table it for this committee, that would be appreciated.

Mr. Ian Scott: We'd be able to give some numbers in the aggregate but not broken down, for the very reason that we don't want bad actors and nefarious players to be able to use disaggregated information to figure out who best to target. To the extent we release that information, we do it on an aggregated basis, if that's acceptable to members.

Mrs. Tracy Gray: That's great. Thank you very much.

Also on that note, can you table for the committee, broken down by month from August 2019 to now, the number of phone porting and SIM-swapping cases of fraud logged by the CRTC as well? Do you have that information?

Mr. Ian Scott: I would have to check. I don't think we would disclose that type of disaggregated information.

Mrs. Tracy Gray: Okay. Do you have general...if it's not broken down in that detail?

Mr. Ian Scott: What I will undertake to do is to look at the numbers we have on an aggregated basis and provide the committee with everything we can, if that would be helpful.

Mrs. Tracy Gray: That's great. Thank you very much.

One of the things you mentioned in your opening address was around AI. This committee undertook a study on quantum computing and how that's emerging. The study is now complete, but there were a lot of concerns brought forth on that, specifically around security risks.

Do you have any information? Is this something you're looking at? We know this is emerging. What impacts could this have in this area we're talking about today with the fraud calls, and are there ways that you're preparing for this?

Mr. Ian Scott: If you're going to ask me to speak to the issue of quantum physics, I think I'm going to duck, and I'm not even sure I could hand that off. I don't even think I can call a friend.

If I can try this, when we approved the trial for Bell and ultimately approved a service, the biggest challenges we received were, one, concerns about privacy and, two, concerns—if you will—about false positives, the potential for blocking out legitimate calls. The trial showed that there were virtually no accidental or erroneous blockages. That's why, after seeing full evidence from the trial, we approved it.

I have not heard of any application beyond that. Nothing has been brought to the commission at this point, but I would suggest that we would approach any such project or proposal the same way that we approached the Bell project. We would want to look at it, have a public proceeding, get the opinions of the Privacy Commissioner and advocates for privacy and any other academic or professional concerns about strengths and weaknesses, develop a record and then make a decision. We're open to every solution the industry and individuals could bring to us. Then we'll have them tested before we allow them to be applied.

I hope that answers the question.

● (1705)

Mrs. Tracy Gray: That's great. Thank you.

It seems, if I'm hearing what you're saying, that you haven't really started on anything like that. It's something that should definitely be on your radar.

Mr. Ian Scott: I have not heard about using quantum computing in this area at all. I'll quickly check with my colleagues.

No, there's nothing to date, but if you have something, we will hear it.

The Chair: Thank you very much.

We'll now move, for our last questioner, to MP Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you, Joël.

Mr. Scott, this was a while ago when we had a different chair. I think Brian and I were members of the committee, and I'm not sure if anyone else here was, when we undertook the study on fraudulent calls in Canada, which was entitled “Fraudulent Calls in Canada: A Federal Government's First Start”. I just want to make sure. Have you and your team reviewed that study?

Mr. Ian Scott: Are you referring to the committee's report?

Mr. Nathaniel Erskine-Smith: That's correct.

Mr. Ian Scott: Yes, we have.

Mr. Nathaniel Erskine-Smith: The government is obligated to respond. The government has responded and pointed to some work it's been doing. There has been credible work to address this issue. In the interest of time, because we don't have much time, would it be possible to get in writing, following up, a clearer sense of the CRTC's perspective in terms of how they have responded, in some cases, to the recommendation, or where the issues were that we were highlighting and how the CRTC is acting in relation to them? Would it be possible to have a more fulsome response in writing that is akin to a response to the report, to go through recommendations where they're relevant to the CRTC so that we have a better understanding of actions the CRTC has undertaken?

Mr. Ian Scott: I'm glad you added the last part.

I would be pleased to undertake a response to describe various measures, as we've tried to do today, that the CRTC has taken that are responsive in some way to the recommendations of the committee. I'd be pleased to do that. You'll understand that it's not my place to respond on behalf of the government, but certainly on behalf of our agency—

Mr. Nathaniel Erskine-Smith: No, exactly. I wouldn't ask you to.

Mr. Ian Scott: —I'd be happy to provide you with a summary of the things we've done that we believe are responsive to issues raised in the report germane to our jurisdiction.

Mr. Nathaniel Erskine-Smith: I would appreciate that.

The only addendum I think is.... I'll use recommendations 12 and 13 as examples in relation to the CRTC. It was a while ago now that we did this. The details of this aren't in front of me at the moment in quite the same way as they were when we went through this the very first time.

Recommendation 12 was:

> That the Government of Canada support efforts by the Canadian Radio-television and Telecommunications Commission to conduct a public inquiry into unauthorized porting.

Recommendation 13 was:

> Should the Canadian Radio-television and Telecommunications Commission fail to launch a public inquiry into unauthorized porting within six months, that the Government of Canada introduce legislation to protect Canadians against unauthorized porting.

You wouldn't have to respond specifically to those recommendations. It would be responding to the question of unauthorized porting and the work you've done in relation to a public inquiry or other work you would have done. That would be the kind of response in writing that I think would be helpful.

The only other question I have is in relation to your work. This is not a uniquely Canadian problem. This is a problem that exists all around the world. You identified it as a challenge in other English- and French-speaking countries. I think you also pointed to Asia being a hot spot for fraud calls.

Are other jurisdictions adopting best practices that you think the CRTC should be seriously looking at? What other jurisdictions around the world would you point to that are addressing this global challenge and doing this better than we are or that are engaging in best practices that we could adopt here at home?

Mr. Ian Scott: Without being immodest, I'd hope that the reason we develop those relationships and partner with those agencies is to learn from them, and hopefully they can learn from us. I think we've been doing that.

I'll be honest. I would say that perhaps the most aggressive and advanced players in this regard are our colleagues south of the border. We have very close contact.

What I would say is that within the confines of our legislative schemes, we have adopted all of the best practices we've identified.

Mr. Nathaniel Erskine-Smith: I appreciate that.

The other thing that would be useful for you to follow up on in writing—and maybe south of the border is the best example—would be where you've identified practices that are worth pursuing, those that other countries are pursuing and that the CRTC is, as a result, pursuing. It would be good for us to understand the work the CRTC has done to improve its own measures with the template being, “We consulted with folks south of the border, and here are steps we undertook to follow their model” or, if that work isn't fully completed in some cases, understanding the status of the work and following through on best practices that you've found in other parts of the world. I think that's very helpful where it's directly relevant to your work.

If in the course of undertaking some of your work—as you say, it's within your legislative scheme—there are other best practices that you come across as a result of your relationships that aren't specific to the CRTC but may be for another agency to pursue, those may also be helpful for the committee's purposes. You might not have a long list, because this is not necessarily within your purview. A follow-up on that in writing would be useful to give a sense of how you are learning from and responding to best practices elsewhere.

● (1710)

Mr. Ian Scott: Thank you. We'll do our best. It's kind of like a progress report and a wish list. I'm not trying to in any way minimize...but I think that's in essence what you're asking for.

I do want to be a bit clear. The two recommendations that you made reference to had to do with porting, which was at the time a growing problem that we were all aware of. An example of that would be that we asked and pushed the industry to do something about it, and they did. They did it without our having to have a public proceeding. The measures they've taken have been successful.

Obviously we have a lot of things to do and a lot of important work to do. We're not going to do a proceeding if we think a problem is resolved or at least on its way to being addressed.

Mr. Nathaniel Erskine-Smith: That's very understandable, and I use that only as an example to say—

Mr. Ian Scott: Understood.

Mr. Nathaniel Erskine-Smith: —that we've identified an issue, and you may identify the way you've addressed that issue, so the recommendation is speaking to something within the CRTC's purview. Then you would respond to us to say, “This is how we've addressed this issue [*Inaudible—Editor*].

Mr. Ian Scott: Understood, and that's exactly.... We're saying the same thing—

Mr. Nathaniel Erskine-Smith: Yes, exactly.

Mr. Ian Scott: —or we're in violent agreement.

I want to say that we have addressed it. We addressed it by telling the industry that we wanted them to address it, and they did, or they are continuing to—

Mr. Nathaniel Erskine-Smith: Exactly.

Mr. Ian Scott: —and that's been good progress.

On the other one, we will do our best, and we'll try to keep our list modest and reasonable.

Mr. Nathaniel Erskine-Smith: Sounds good. Thank you.

Mr. Ian Scott: I appreciate the question in terms of what we can do better and what other practices we could apply if we had some additional flexibility, and we'll take it in that spirit.

Thank you for that.

The Chair: Thank you, Mr. Scott.

Thank you, Nate.

We still have a bit of time, and I know that MP Dong has I think one or two more questions.

You can go ahead, MP Dong.

Also, if anyone else has more questions....

Mr. Ian Scott: If he's going to ask about quantum computing, I'm leaving.

Voices: Oh, oh!

Mr. Han Dong: Actually, it was my motion to study quantum computing, but I won't ask about that today.

I'm just trying to get my head around how to break down the silos you were talking about. If Rogers or BeIl spots some suspicious activities, are they allowed to pass that on? Are they required to pass on that information to the CRTC? Otherwise, how would you know that there are suspicious activities going on? They're the service providers, right?

Mr. Ian Scott: That's a very complicated question, more complicated than you might imagine.

Carriers can do certain things. I'll use the example of malformed phone numbers.

Mr. Han Dong: I'm just talking about fraudulent calls.

Mr. Ian Scott: I do want to—

Mr. Han Dong: They receive a complaint from the customer—

Mr. Ian Scott: It's not a question of complaints here. We're talking about—or at least what I was talking about—actions the companies can take when they know there are things coming across their system that may be fraudulent. They have to be careful because, under the Telecommunications Act, they're not allowed to influence the content of the messages. From a privacy perspective, and just a civil society perspective, we don't want phone companies poking inside the messages and going, “I don't think we should let that one through, but this one is okay.”

Mr. Han Dong: Right, yes, but when they tag this as a possible fraudulent call—

Mr. Ian Scott: Then they would have to come to us. The example of how Bell developed a potential approach to deal fundamentally with what we call callback schemes to generate revenue from international accounts—

● (1715)

Mr. Han Dong: So they would—

Mr. Ian Scott: They have to come to us and say, “Can we apply this technology?” In that case, they said, “Could we do a trial and apply this technology to see if we can screen out calls in this way?” We gave them permission to do it on a temporary basis following a public proceeding where we got input, and then we gave it a permanent approval because they demonstrated that there were not errors and it was effective—

Mr. Han Dong: What do they do when they spot something, when they catch something that might be a criminal fraudulent call?

Mr. Ian Scott: We have to separate criminal from what they believe are not—

Mr. Han Dong: Sorry, not criminal, but legitimate calls, yes—

Mr. Ian Scott: Yes: legitimate calls or patterns—

Mr. Han Dong: What would they do?

Mr. Ian Scott: What they should be doing.... As I said, it's a delicate question. Can they take some measures on their own? They might, but they have to be very careful, because there are very clear lines drawn in the—

Mr. Han Dong: Let me ask you this—

Mr. Ian Scott: They have to come to us and ask us.

Mr. Han Dong: If they can give this information to you or tag the information about these calls, why can't they give that information to the RCMP?

Mr. Ian Scott: If I'm understanding the question, we're mixing different concepts.

They don't know that it's a fraudulent call. What we're dealing with here, if we took spoofing.... Actually, I'll go back to the Bell example. That's a system where they're getting callbacks. They're calling numbers, and then they get a callback because people do it automatically, and then they get money.

People are making money on the international accounting settlements. I won't go into the details, but they're irregular. You shouldn't be getting thousands of calls from “a place”. It's the pattern of calls that you're dealing with.

Mr. Han Dong: Okay.

Mr. Ian Scott: That is when they'll come and say, “We're seeing this pattern, and we know they're not legitimate calls.”

Mr. Han Dong: Under the current legislation, can they go to the RCMP and say the same thing?

Mr. Ian Scott: They could, but they don't know what's happening. They don't know. They can't go inside those calls and listen or know what's going on. They're coming to us, as the regulator, to say, "We think these calls are illegitimate and we want to take measures."

Mr. Han Dong: That's not my question. My question is, under the current law, can they go to the RCMP?

Mr. Ian Scott: They could go to the RCMP, but they would be telling them that they're getting a whole bunch of calls using this number pattern, which doesn't mean anything to the RCMP. It means something to us.

Mr. Han Dong: The reason for my question is that we'll be seeing the RCMP on Monday. I'll ask the same question.

Mr. Ian Scott: They couldn't deal with that.

I'll just very quickly go back to the idea of malformed numbers. If you're getting numbers that aren't real phone numbers, full of a bunch of zeroes because scammers are sending calls through the system using phony numbers, or they're all fives or they're all fours, it doesn't matter what it is; they know it's not a real call. If that goes to the RCMP.... It's not a crime to try to use all fours to go through.

Mr. Han Dong: I'm trying to find a way to break down silos and really understand what we can do in order for information to flow. Today we're hearing from you that you are not a law enforcement body. You want to pass on this information. I'm sure the RCMP will say it doesn't have access to this information. There is a door in between the two agencies. Who's going to open that door?

What I'm saying is—

Mr. Ian Scott: I agree, and maybe Steven can speak briefly to the information.

Mr. Han Dong: My point is that you don't collect information. You're not a service provider. The service provider is flagging these calls to you. I don't understand. You just explained the pattern. It's a different issue.

Mr. Ian Scott: It's a different issue. They're flagging to us that these are malformed numbers or whatever. Our intelligence group is flagging things like how there's a spam campaign; there's a campaign going on that looks as though it's fraudulent. We see it. We're getting complaints. They come to the spam reporting centre. Our intelligence group identifies, perhaps, where they're coming from.

Steven, you can add to this. That's the stuff we want to report to the RCMP, that we think there's a fraud campaign going on.

Mr. Han Dong: Currently you can't do that?

Mr. Ian Scott: Well, we can to a point.

Steven.

Mr. Steven Harroun: We can in aggregate. That's what we share with our telcos around those calls as well as with the RCMP and the Canadian Anti-Fraud Centre. We share aggregate information about campaigns we're seeing, campaigns the telcos are seeing.

To your specific question earlier, I'm well familiar with the TSPs and the fraud departments they have and the number of resources they have. I am certain that if they have complaints from a particular customer on being victimized, etc., there's a process for them to deal with those. Either the complainant can deal with them with law enforcement officials or Rogers may or may not—I use that name vicariously—with the RCMP as well.

If there are specific complaints of someone having been victimized, then there are methods of dealing with those, of course, through the criminal system. The challenge we face, even as the CRTC, is that we are seeing these campaigns, these types of things, that we pass along. For our colleagues at the RCMP, whom we appeared beside the last time, in March, that is one pile out of a very much bigger pile of cases they have to look at.

I'm sure there are ways, but for us there are details we can't share. We can share aggregate information. We can get everybody on a call saying, "Yes, we're seeing this type of activity, these types of things", but we can't share the specifics.

To your point that a customer from Rogers, Bell, Telus or whoever is being victimized, we're sure there is a process for them to deal with that as well, but that's very separate from us. That goes to your criminal point.

● (1720)

The Chair: Thank you, Mr. Dong.

Thank you, Mr. Harroun.

We'll move to Mr. Lemire.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much, Mr. Chair.

I'd like to begin by complimenting Mr. Masse for his leadership on this matter, which we have before us again. And a nod to Mr. Erskine-Smith to let him know that I too was there when we studied this matter two years ago. It just goes to show you how quickly things move in Parliament.

I have a question for the witnesses about recommendation 9 from the committee's most recent report on this matter, which reads as follows:

> That the Government of Canada encourage the Canadian Radio-television and Telecommunications Commission to monitor and consider the cost of industry-based solutions against fraud calls when making decisions that affect the affordability of telecommunications services.

Are you worried that the cost of protections against fraud calls will be passed on to consumers?

Mr. Alain Garneau: The information we received in response to our consultation notices didn't raise any concerns about that. Most of the time, the costs involved are tied to network operations, and having these comply with the decision would not generate any additional costs.

When the Canadian Radio-television and Telecommunications Commission asks the industry to do certain things, it usually show some reluctance at the outset. However, it usually comes around very quickly because it understands that it's not necessarily always a matter of costs, but benefits as well. This is also profitable to the industries, not only because there will be fewer calls of this kind clogging up their networks, but also because of the better service to their customers. In the end, the market will dictate which are the best or the most proactive.

There are therefore not really any costs involved in these measures, except perhaps for a social cost.

Mr. Ian Scott: With your permission, I'd like to add something.

[*English*]

It may have been Mr. Masse who raised this in previous meetings, but I think there's a concern, as we impose constraints or direct phone companies to take measures, that we need to be very attentive to: that those costs of implementing those measures are not immediately passed on to consumers. I think that's a very important point and one that we're paying close attention to.

Thus far, I have not seen any measures that the companies have introduced where they are saying, “We can protect you. We have a great new gadget approach that will get rid of most of the spam calls, and it's only an extra $2 a month on your cell bill or on your phone bill.”

We have not seen that. I can at least speak for myself to say I wouldn't be very supportive as a regulator of such an approach by the carriers. I think it is in their interest to address this, and they should compete with one another for their customers in part on how well they protect them and serve them, not just their quality of service or their coverage, but also in things like protecting them from unwanted communications. I think it's in their best interest, but also, we should make sure it's not at the expense of consumers.

I think that's part of what underlies that. I'm not being very subtle, but I can say that I would not be supportive of seeing.... Let me rephrase it: I have expectations that the industry should deal with this because it's in their best interest and the best interest of consumers.

● (1725)

[*Translation*]

Mr. Sébastien Lemire: Thank you.

You've answered my question and my subsidiary question.

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

So that's the end of our meeting today.

Thank you Mr. Garneau, Mr. Scott and Mr. Harroun for having joined us today. The committee would appreciate it if you could submit to us in writing the commitments you have made and the answers you've promised.

On that note, I wish everyone a good evening.

The meeting is adjourned.