# Chairman Jean-Pierre Blais speech on how the CRTC is improving the security and safety of Canadians given at the Economic Club of Canada

**Toronto, Ontario**
**June 26, 2014**

**Jean-Pierre Blais, Chairman**
**Canadian Radio-television and Telecommunications Commission**

**Check against delivery**

Thank you for your kind words of introduction. I am flattered to have been invited to meet with you, given the Economic Club of Canada's envious reputation as the "National Podium of Record."

I welcome this opportunity to go on the public record about an issue that matters not only to those of you in this audience, but to all Canadians.

No, I'm not talking about the Let's Talk TV conversation we have been engaged in since last fall – although the future of television in this country is certainly of great interest to Canadians and the broadcast sector alike. Our public hearing on Let's Talk TV kicks off on September 8th.

Perhaps you came here this morning expecting an update on our review of the mobile wireless services market – another important subject for Canadians and the telecom sector. Our hearing on this issue gets underway on September 29th. However, that's not the subject of my talk today either.

Neither am I here to discuss fibre-to-the-home and the need to reinvest in our telecommunications networks. We've scheduled a hearing on wholesale telecommunications services for November 24th.

All three hearings go to the heart of the economics of the $60 billion communication sector in Canada – but that will be a discussion for another day.

Instead, I want to talk about how the CRTC is fundamentally transforming to respond to the impacts of the technological changes taking place in these sectors.

## Life in a digital world

We live in a time when our communication system has become a lifeline for most of us. Powerful digital communication devices and services are ever-present in our lives. They bring entertainment, information and business tools—wherever Canadians live and work.

They provide unprecedented connectivity to friends, family, colleagues, governments, businesses and customers. Wherever we are. From cars to classrooms, from buses to boardrooms and from living rooms to sports fields.

And, in a very real way, the regulatory presence of the CRTC accompanies those communication devices and services. In fact, I sometimes say that, to the extent that Canadians bring their radios, televisions, telephones, smartphones and tablets to bed—as many of us do—the CRTC is one of the rare government institutions that IS in the bedrooms of the nation!

We can joke about it but, the fact is, technology is now an integral and ubiquitous part of our daily lives. This reality brings with it new responsibilities for the federal regulator. Just as the world of communications is changing, so must we. And that's what I want to focus on this morning.

Because, as the respected U.S. jurist, Francis T. Murphy, once remarked,

> "No more essential duty of government exists than the protection of the lives of its people. Fail in this, and we fail in everything."

## Protecting the public interest

People tend to think of the CRTC in terms of broadcasting and telecommunications—ensuring Canadians have access to a world-class communication system.

It's true that much of our work revolves around making sure Canadians can access compelling broadcasting content from diverse sources and on a variety of platforms. And that they can connect to high-quality and innovative communication services at affordable prices.

But there is another, equally important part of our work that extends beyond addressing the needs of content creators and consumers.

That's our responsibility to protect the public interest for all citizens—to harness technology's potential to do good and to minimize its power to do harm.

There are few jobs, few sectors and few aspects of our lives that remain untouched by digital technologies. Therefore, the integrity of the system must be

continually maintained and enhanced.

It's our job to make sure citizens can enjoy peace and quiet in their homes and a more secure online world. This means making sure the telephone calls they receive are from legitimate telemarketers who follow the rules. And that they can open their email without having their identity or intellectual property stolen.

We also ensure citizens can connect to a 9-1-1 call centre in an emergency and receive assistance or timely warnings, such as when severe weather is expected.

## Evolving role

This is a role we don't take lightly at the CRTC. Neither does the federal government, which has introduced new legislation to protect the public interest.

Parliament has updated the CRTC's mandate with initiatives like the National Do Not Call List and Canada's anti-spam legislation. The recently passed *Fair Elections Act* also gives us the authority to establish a voter contact registry.

These changing responsibilities are altering our organization. Gone are the days when our jobs centred on issuing broadcasting licences, setting policy frameworks and reviewing ownership changes.

When I worked in the CRTC's Legal sector in the 1990s, we had to review and approve tariff applications for virtually all telephone services. We were also heavily involved in the regulation of television and radio services.

Today, the majority of the retail telecommunications services used by Canadians have been deregulated because healthy competition in the marketplace replaces the need for regulatory interference. All retail telecommunications services brought in total revenues of about $40 billion last year. Over 90% of that amount now derives from deregulated retail services.

We still develop policies and regulations, of course. But our enforcement officers are just as likely to knock on the door of a duct cleaning company or robocall firm to conduct an on-site inspection. They have shields and uniforms. And they utilize cutting-edge investigation techniques to serve and protect Canadians.

## New powers

The CRTC has a range of tools as its disposal to ensure compliance with the Unsolicited Telecommunications Rules, the voter contact registry and Canada's anti-spam legislation. These include investigative powers, preservation demands and warrants, information sharing with partners to assist investigations and the powers to impose heavy administrative monetary penalties.

Anyone questioning why the Commission would need such powers needs only consider that there are now apps to disclose the private telephone numbers of women's shelters to known abusers of their residents.

A respected business's reputation can be destroyed when irate customers mistakenly believe they are being harassed by the firm. That's what can happen when callers conceal their true identity by using someone else's legitimate phone number—a practice known as caller ID spoofing.

More damaging is the handiwork of malware disseminators and phishers, many operating offshore. They can clean out a Canadian's bank account by discreetly capturing key strokes or with convincing e-mails that lead an unsuspecting person to think they're dealing with their neighbourhood financial institution.

There is clearly a time and place for government to step up to protect citizens' health and safety and the security of Canada's economy. If governments do not act, public confidence in the communication system risks being undermined. Would you not be tempted to unplug your phone if eight out of 10 calls you receive are unsolicited telemarketing calls?

The CRTC is well on its way to implementing a framework to uphold Canadians' right to peace and privacy in their homes, undisturbed by unwanted calls. To give people confidence they can safely work, shop and communicate online because the digital environment is secure and reliable. And to make Canadians safer in times of emergency.

## National DNCL

The National Do Not Call List is a perfect illustration of both the CRTC's new role and how quickly things are changing in the world of technology. And how challenging it is to stay on top of it. While not life threatening, telemarketers' ploys can do serious damage.

As you likely know, Canadians who sign up for this service have made a deliberate choice to **not** receive unsolicited telemarketing calls.

Canadians have registered more than 12 million numbers on the list. That's about 29% of Canadian households. They continue to do so at a rate of 1,200 new numbers a day.

I'm happy to reiterate yesterday's announcement that all registrations to the National Do Not Call List are now permanent. Canadians no longer have to worry about having their registration expire and their phones lines unexpectedly flooded with telemarketing calls.

More than 10,000 telemarketers subscribe to the list too—not only from Canada, but also the United States, India and other countries.

It's important to keep in mind that certain groups are exempted from the List, such as registered charities, political parties and companies conducting surveys or selling newspapers.

There's a reason for this. We must not eliminate these sectors' ability to communicate with the public or deny them freedom of expression. This is essential in a democratic society. That said, these groups are nevertheless obliged to have—and respect—internal do-not-call lists.

The legislation sought to strike a balance between the interests of telemarketers and the privacy of Canadians—something we strive to do in all of our deliberations at the CRTC.

When telemarketers fail to respect the privacy of Canadians, the Commission can investigate and take action. To date, we have levied nearly $4 million in penalties from telemarketers that violated the Unsolicited Telemarketing Rules.

We have engaged in more than 1,200 investigations. And we have issued numerous citations, compliance letters and notices of violation.

In 2013-2014 alone, we took enforcement actions against telemarketers responsible for over 11 million calls to Canadians that were in violation of the rules.

Now, I realize that sounds like a lot of calls. And I know that some people consider it a failure if just one annoying call gets through. To them, a telemarketing call is not just a dinner-time disturbance. It is an invasion of their privacy. Canadians who register their numbers fully expect they won't be bothered anymore.

But the reality is, Canadians were spared from calls they would have received were they not registered on the National Do Not Call List. A survey conducted by the Marketing Research Intelligence Association in 2012 found 78% of people on the list reported receiving fewer calls. So much for the urban legend that people get more calls now than before signing up.

Between the exemptions built into the legislation and the rogue telemarketers who ignore the rules, we will never be at a point where there are zero unsolicited calls. We need to make sure we set realistic expectations for the National Do Not Call List.

Malicious telemarketers are especially problematic. They exploit vulnerabilities in the system to hide their identities and call Canadians repeatedly at all hours. Sometimes, these callers attempt to deceive them to obtain their credit card information or to sell people ineffective or useless services.

We get countless calls and emails from frustrated Canadians who are at their wit's end. Even the most meek, mild and polite Canadians have had enough.

Here's an example of a note I received from Elizabeth in Barrie, Ontario:

> "We get a "DAILY" harassment phone call from a duct cleaning company. We have informed them we are on the do not call list, we have asked them not to call, politely and not so politely. We have threatened them with legal action, they still continue to call us – and as late as 9:30 p.m. What can be done to stop these annoying calls?"

And another typical complaint from the other side of the country—this time from Norm, in Shawnigan Lake, British Columbia writes:

> "We are on the Do Not Call List and received a phone call at 12:59 a.m. They wanted me to press 1 to speak to an operator to lower my credit card interest rate. I pressed 1, and then when a person answered I asked 'why are you calling me when I'm on the Do Not Call List?' He claimed I called him! Why are they allowed to phone my private residence when I'm registered to not receive these calls?"

As irritated as the person receiving the calls may be, pity the poor victim whose number is spoofed. There was a recent case in Ottawa where an innocent person was inundated with harassing calls from hundreds of angry people who had been contacted by a telemarketer using her number.

So what is the CRTC doing to get at these rogue telemarketers?

First, we have been in discussions with our law enforcement partners here in Canada as well as telecommunications companies to evaluate how to address this growing problem.

## International cooperation

However, there are limits to what we can do domestically, given that these calls come from all over the world. Telemarketers, like hackers and spammers, often operate outside our borders.

That's why we collaborate with our international counterparts—the Federal Trade Commission in the U.S., the Office of Communication (OFCOM) in the U.K., the Authority for Consumers and Markets in the Netherlands, the Australian Communications and Media Authority and others.

We've led or participated in many international networks. We were one of the co-founders of the International Do Not Call Network and are an active member of the London Action Plan. Both these groups were created to foster greater cooperation on cross-border issues.

We are also working with telecommunications service providers and the Messaging Anti-Abuse Working Group to step up our efforts to find rogue telemarketers. The CRTC took part in the Group's first voice and telephony anti-abuse workshop in February as well as a follow-up meeting held last week in Montreal.

We focused on a range of possible solutions to stop these types of abuses and to overcome the hurdles to implementing them. We are exploring proactive approaches to foresee abuses or attacks, monitor them and take enforcement actions before they reach consumers.

For instance, we are creating voice telephony honeypots to lure rogue telemarketers so we can catch them in their deceitful webs. These so-called honeypots involve a series of numbers, along with call routings, that are being given to regulators in various countries by telecommunications companies. We would use them to monitor all incoming calls in our respective jurisdictions and better target our enforcement efforts. We hope to have more news on this front later this summer.

We are also exploring trace-back programs, call-blocking policies and abuse reporting.

Another area of shared concern with our international partners is how people report calls made using spoofed numbers.

We are working in partnership with the private sector on a system that would let Canadians press a number on their phones after receiving a spoofed call to automatically forward the information to the CRTC for follow-up. Something along the lines of the Star 09 or Star 69 services you may be familiar with.

We are determined to beat the bad guys at their own game by developing a technology solution to a technology problem. Because we recognize there's no putting the genie back in this bottle.

This is not something we can do alone. Given that the industry has a pivotal role to play in maintaining the integrity of the system, I expect that it will rise to the challenge.

It's in the business community's best interests to do so. Because the public interest is, ultimately, a shared responsibility.

## Voter contact registry

The CRTC's experience with the National Do Not Call List has given the federal government the confidence to assign new responsibilities to us.

Under the *Fair Elections Act* that Parliament recently adopted, we were given the authority to establish and maintain registration information for voter contact services. This is critical to protecting Canadians' democratic rights.

We will be ready to implement the voter contact registry in time for the 2015 federal election. We will be conducting outreach activities to ensure candidates and voter contact services are aware of their new responsibilities and to provide information to the public.

This new registry reinforces the central role citizens play in the CRTC's mandate and just how seriously we take this responsibility.

## CASL

We are also the primary agency responsible for ensuring compliance with Canada's anti-spam legislation.

Now, I suspect many of you have had a flurry of emails over the past weeks. Everybody—from your accountant and real estate agent to online retailers—is asking for your consent to continue receiving messages from them. I have been receiving an average of five a day. Do not despair. This is the final unregulated rush as companies prepare for the law to come into force on July 1st.

Once it is in force, this new law will protect Canadians while ensuring businesses can continue to compete in the global marketplace with the assurance of a secure online environment.

As business people, you know better than anyone the damage that hackers can do. You recognize just how dangerous spyware, malware and phishing are to your operations and how seriously they can hurt your brand.

Once these programs are installed on a computer, spammers can steal personal data, defraud individuals and corporations, and disrupt the legitimate flow of information across electronic media.

The new federal strategy, Digital Canada 150, reports that 32% of computers worldwide were infected with malware in 2012. There was a 600% increase in the number of websites hosting malware from the year before.

Even more alarming, the Washington-based Center for Strategic & International Studies recently reported that cybercrime costs the global economy US$400 billion each year. The impact on the Canadian economy is estimated at US$3.2 billion.

All of this chips away at Canadians' confidence in e-commerce, at great cost to your companies and the economy at large. That's a serious problem given that Canadians are among the lowest users of e-commerce in the G7.

Canada is ranked as 2nd in Internet penetration among its G7 counterparts. But Canadians spend less online than citizens in other countries. The value of e-commerce in Canada was $22.3 billion in 2013.

That may sound impressive, but a 2012 study shows that e-commerce accounted for only 3.4% of total spending in this country. Compare that to 7.1% in the U.S and 23% in the United Kingdom that same year.

A more secure environment is not only good for citizens. It is equally good for business.

So we will be going after the most egregious violators: the high-volume spammers, the malicious URLs and the botnets located in Canada.

Under Canada's anti-spam legislation, or CASL for short, the Commission will investigate individuals and organizations for:

- sending commercial electronic messages without prior consent, that do not have an unsubscribe mechanism or that do not include identification information
- altering transmission data without a recipient's permission – for example, directing Internet users to a website they did not intend to visit, and
- starting in January 2015, installing a program or application on a computer system or network without the individual's express consent.

It will be against the law to use false or misleading representations online to promote products or services, to collect personal information through accessing a computer system, or to harvest addresses without permission.

These rules not only apply to email but to all electronic messages – text messages, message on social networks and other forms of electronic communications.

Basically, anyone who sends commercial messages to Canadians will need to comply with the law.

As of next week, Canadians can start reporting spam and other electronic threats to the Spam Reporting Centre. It will serve as a clearing house for complaints that will be assigned to the CRTC, the Competition Bureau or the Office of the Privacy Commissioner for assessment and appropriate action.

The CRTC has a team of highly-qualified people ready to start enforcing Canada's anti-spam legislation. We have former RCMP officers, major criminal investigators and sophisticated computer forensics experts who will be leading these efforts. Enforcement is now in the CRTC's DNA.

Beyond additional personnel, we have state-of-the-art facilities in our new cyber-forensics lab—an in-house centre designed and built by the country's foremost technology leaders. The lab will enable us to search, seize and copy digital evidence that proves violations of the new law to better protect the public.

Our electronic commerce enforcement specialists will be able to search and index tens of millions of messages and reverse engineer malware to trace the source of these scams and follow their online links.

We have some serious financial clout too. The CRTC will be able to issue penalties of up to $1 million for an individual and up to $10 million for a company per violation. As of July 1, 2017, individuals and organizations affected by a contravention of the law will be able to take court action to seek actual and statutory damages.

Similarly, I am pleased to note that, last December, the Minister of Industry announced that the government intends to amend the *Telecommunications Act* to give us the power to impose monetary penalties across all our telecommunications activities. I look forward to seeing that legislation enacted in the coming months.

Once in place, it would mean, for example, that we could assign penalties if a service provider did not follow requirements related to the 9-1-1 system, or if a wireless provider contravened the wireless code.

We've seen a few over-the-top reactions to these new powers from folks who are convinced we are out to get them. We have heard concerns that we will start imposing significant penalties for even the smallest violations.

I want to say a few things about this. First, CASL is the law. It was passed by our elected representatives in Parliament. The CRTC has a duty to implement it.

Second, as I alluded to earlier, we have more than enough human and technical resources to do whatever is needed to ensure the law is upheld.

Third, and more fundamental, punishment is not our goal. We are not going to go after every indie rock band that's trying to sell a new release to its fans. We have much bigger fish to fry.

The CRTC will focus on the most severe types of violations. This means you may still receive the occasional spam message after July 1st. Our principal targets are abusive spammers and interlopers involved in botnets and, come January, malware and malicious URLs.

Our responses to complaints will range from written warnings up to financial penalties or court actions. Our objective is to secure compliance and prevent recidivism. I believe the best enforcement approach should be determined by the facts surrounding each particular case.

My final point is simply this: if you abide by the law you have nothing to fear. Good corporate citizens will be in good standing.

Now, I realize there's the potential for the law to become known as the 'unemployed lawyers relief act' if companies choose to fight these changes. But I would strongly urge corporate leaders to get with the program.

Ultimately, Canada's anti-spam legislation, like the proposed changes to the *Telecommunications Act*, is about creating a better, safer, more trusted environment to do business.

## 9-1-1

I have gone on at length about protecting the public interest and I haven't even touched on 9-1-1 services – the very epitome of why Canadians need a reliable and modern communication system.

If I had more time, and you didn't need to run to the office, I would tell you about the next generation of 9-1-1 services.

There is no question we need to update the system so Canadians can communicate with 9-1-1 call centres using different media—things like text messages, pictures and videos.

We have just released our action plan to enhance existing 9-1-1 services and ensure that telecommunications networks are ready to support next-generation 9-1-1 services. You can find a fact sheet on this topic on our website.

This is a complex issue involving many players. This includes multiple departments in multiple levels of government—federal, provincial, territorial and municipal—as well as call centres and emergency responders.

Some have suggested that greater coordination between the different partners could be achieved through a national forum. We would be prepared to participate in such a forum and share our expertise in the areas under our jurisdiction.

I can attest to real-life examples I come across in my work which underscore why having a secure and reliable communications system is vitally important. It is, quite literally, sometimes a matter of life and death.

One of the most difficult parts of my job is receiving copies of coroner's reports that describe someone losing their life because emergency responders were unable to locate the person quickly enough. These cases illustrate how Canada's communication system—**our** communication system—can —and must—do better.

## Conclusion

Situations like these also underline the difficult balance that CRTC Commissioners must work to achieve as we juggle the interests of consumers, creators and citizens.

We prefer to be unobtrusive in the marketplace whenever possible. Yet we have new legal obligations to put an end to harmful activities that threaten the lives and livelihoods of Canadians.

No matter what, we must look out for the public interest, which overrides all other considerations. While the market will generally address the needs of most consumers, it will not always address those of citizens.

And, as Thomas Murphy said, if we fail in this, we fail in everything.

We are seeing a new CRTC emerge as we take on a greater enforcement role. In future, we will play a more active part in meeting head-on the challenges that come with fast-changing communications technologies.

But this isn't just the Commission's domain. Protecting the public interest is something we all need to take seriously, given the high stakes in today's highly connected world. We have a collective interest in, and responsibility to, make sure new technologies do good, not harm—for the good of us all.

The public sector, the private sector and non-governmental organizations all have a contribution to make in ensuring Canadians' communication system upholds their rights and interests, and protects their health and safety.

I look forward to working with corporate leaders like you as we do just that.

Thank you.

**Date Modified:**

2014-06-26