**Questions from the UN Special Rapporteur on the**

**promotion of the right to freedom of opinion and expression**

1. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:

1. Suspend or restrict access to websites or Internet and telecommunications networks
2. Provide or facilitate access to customer data;

2. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to (a) suspend or restrict access to websites and telecommunications networks and the requests to provide or (b) facilitate access to customer data;

3. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points;

4. Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data;

5. Other relevant laws, policies or initiatives to promote or enhance Internet accessibility and connectivity, including measures to promote network neutrality.

**1. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:**

1. **Suspend or restrict access to websites or Internet and telecommunications networks**

***Telecommunications Act* (TA)**

Section 36 of the TA states specifically that Canadian telecommunication common carriers “shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public” except as approved by the Canadian Radio Telecommunication Commission (CRTC). The CRTC has in the past provided some valuable guidance with respect to section 36 of the TA. In Telecom Regulatory Policy 2009-657, the CRTC reviewed the Internet traffic management practices (ITMPs) of Internet service providers and found that an ITMP that led to the blocking of the delivery of content to an end-user would engage section 36 of the TA and, consequently, would require the prior approval of the CRTC in order to be implemented. The CRTC also stated that such an approval would require exceptional circumstances and would only be granted where it would further the telecommunications policy objectives set out in section 7 of the Act.

It is noteworthy that the CRTC may issue an order pursuant to section 42 of the TA to require or permit any telecommunications facilities to be provided, constructed, installed, altered, moved, operated, used, repaired or maintained or any property to be acquired or any system or method to be adopted, by any person interested in or affected by the order, as the CRTC determines to be just and expedient. Similarly, pursuant to section 51 of the TA, the CRTC may order a person, at or within any time and subject to any conditions it determines, to do anything the person is required to do under the Act (or any special Act), and may forbid a person to do anything that the person is prohibited from doing under the Act (or any special Act). We’re not aware of any instance where those provisions have been applied to suspend or restrict access to websites or Internet and telecommunications networks.

Full text of the *Telecommunications Act* is available at <http://laws-lois.justice.gc.ca/eng/acts/t-3.4/FullText.html>.

***Copyright Act* (CA)**

Certain provisions of the CA may qualify as measures that under specific circumstances permit authorities to require Telecommunications and Internet Service Providers (TISPs) to suspend or restrict access to websites and, or to provide access to customer data.

The so-called “Notice and Notice” regime was introduced in January 2015 to strengthen the ability of copyright owners to control the use of their online works. In cases when copyright owners claim that an Internet user might be infringing their copyright, they can send a notice of alleged infringement to the user's Internet service provider (ISP). Notice and Notice requires that the ISP forward (e.g. via email) the notice of alleged infringement to the user and then inform the copyright owner once this has been done. In case of a claimed infringement of copyright the copyright owner “is not entitled to any remedy other than an injunction against a provider of an information location tool that is found to have infringed copyright by making a reproduction of the work or other subject-matter or by communicating that reproduction to the public by telecommunication” (section 41.27(1) of the CA). The term “information location tool” has been defined in the CA as any tool that makes it possible to locate information that is available through the Internet or another digital network. An ISP would thus only be suspending or restricting access to an infringing web site if ordered to do so by the court.

Moreover, section 2.4(1)(b) of the CA provides, in effect, that providers of telecommunication services who act only as conduit for the communication of a work to the public, and do not themselves engage in acts that relate to the content of the communication, are protected from liability for breach of a copyright caused by the communication.

***Criminal Code* (CC)**

Several *Criminal Code* provisions allow a judge to issue a warrant of seizure to make sure that specific materials relating to terrorist propaganda (section 83.223 of the CC), child pornography, voyeuristic images and intimate images (section 164.1 of the CC), or hate speech (section 320.1 of the CC) are “no longer stored on and made available through the computer system”, which may in effect suspend or restrict access to websites publishing such materials.

***An Act respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service* (MRICP)**

The MRICP is intended to fight Internet child pornography by requiring Internet service providers and other persons providing Internet services (e.g., Facebook, Google and Hotmail) to report any incident of child pornography. This requirement includes the following:

* If a person providing Internet services is advised of an Internet address where child pornography may be available, the person must report that address to the organization designated by the regulations.
* If a person has reasonable grounds to believe that the Internet services operated by that person are being used to transmit child pornography, the person must notify the police and preserve the computer data.

While the notification requirement is not a power to suspend or restrict access to telecoms services *per se*, it may be surmised that the reporting may lead to restricting access to child pornography websites. According to section 164.1 of the CC, a judge may order an ISP to provide information to identify and locate the person who posted the website. It may also order an ISP to remove the child pornography in question from the Internet.

**Recent provincial legislative proposals**

While our expertise is in the applicable federal legislation, it is worth noting that a recent provincial legislative initiative is using restrictions on access to certain websites as an enforcement tool. The Québec government enacted last May amendments (through Bill 74) modifying  its *Consumer Protection Act* to require Internet service providers to block access to online gambling sites identified by Loto-Québec (see <http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2016C7A.PDF>, sections 13 to 18 in particular). However, the constitutionality of these amendments  is being currently challenged before the Superior Court of Québec and the CRTC. In a Telecom Commission Letter Addressed to Distribution List and Attorneys General, dated September 1, 2016 (available at <http://www.crtc.gc.ca/eng/archive/2016/lt160901.htm>), the CRTC expressed its view that it is exclusively responsible for the administration of Section 36 of the TA and will remain so, regardless of any finding with respect to the constitutionality of Bill 74. It further stated that the TA prohibits the blocking by Canadian carriers of access by end-users to specific websites on the Internet, whether or not this blocking is the result of an Internet traffic management practices and that any such blocking is unlawful without prior CRTC approval, which would only be given where it would further the telecommunications policy objectives. Thus, in the opinion of the CRTC, ”compliance with other legal or juridical requirements—whether municipal, provincial, or foreign—does not in and of itself justify the blocking of specific websites by Canadian carriers, in the absence of Commission approval under the Act.”

**1. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:**

1. **Provide or facilitate access to customer data;**

***Telecommunications Act***

Based on section 37 of the TA, the CRTC may request from the Canadian telecommunication carriers certain information that may conceivably contain some broadly understood customer data either in periodic reports (which may conceivably contain information about the number of customers in certain areas, use of data networks, etc.) or other information provided to CRTC as “necessary for the administration of the Act”. As a general rule, the CRTC is obligated to make such information provided to it available for public inspection (section 38). However, section 39 of the TA ensures that confidential information designated as such by the Canadian carrier will be protected from disclosure (subject to narrow exemptions).

Moreover, offering and provision of any telecommunications services by Canadian carriers is subject to standard *Terms of Service* adopted by the CRTC (under section 24 of the TA). Article 11.1 of those *Terms* provides that, a disclosure of customer data is possible if it is required pursuant to “legal power”. Otherwise (unless a customer gives an express consent) all information kept by a carrier regarding the customer, other than the customer’s name, address and listed telephone number, is confidential and cannot be disclosed by the carrier to anyone (except the customer, customer’s agent or another telephone company provided the information is required for efficient provision of telephone service and the disclosure is made on confidential basis with the information to be used only for that purpose).

In Telecom Decision CRTC 91-2 *Criminal Intelligence* *Service of Ontario-Release of Information by Bell Canada*, the CRTC refused the request to permit the release of “information kept by Bell Canada regarding the customer”. However, in Order 2003-319 the CRTC approved an amendment to Bell’s Terms of Service allowing for disclosure (without express consent) to a public authority, if in the reasonable judgement of Bell it appears that there is imminent danger to life or property which could be minimized or avoided as a result of the disclosure.

**Canada’s Anti-spam Legislation (CASL)**

Under CASL (“An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act”), the CRTC may order telecommunications service providers to preserve transmission data that is in or comes into their possession or control (CASL, s. 15), and require production of documents by a person to determine compliance with CASL (CASL s.17). Additionally, warrants may be issued by a justice of the peace to verify compliance with CASL (CASL, s.19).

It is noteworthy that these powers may be used to assist an investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct prohibited under any of sections 6 to 9 (CASL, s. 15(3), 17(2)(c) and 19(a)(iii)).

Full text of the CASL is available at <http://laws-lois.justice.gc.ca/eng/acts/e-1.6/fulltext.html>.

***Criminal Code***

In addition, the recently amended the *Criminal Code* contains several provisions permitting in very limited circumstances the authorities to require the TISPs to provide or facilitate access to customer data.

Under section 487.012 “[a] peace officer or public officer may make a demand to a person in Form 5.001 requiring them to preserve computer data that is in their possession or control when the demand is made."

Section 487.014 deals with general production orders which allow the court to order a third party to produce records, including those related to the identification of a subscriber (customer) under the following conditions:

**(2)** Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to believe that

**(a)** an offence has been or will be committed under this or any other Act of Parliament; and

**(b)** the document or data is in the person’s possession or control and will afford evidence respecting the commission of the offence.

Moreover, the newly added section 487.017 allows the justice or judge to order a person to prepare and produce a document containing tracking data that is in their possession or control when they receive the order if the judge or justice is satisfied there are reasonable grounds to suspect that:

**(a)** an offence has been or will be committed under this or any other Act of Parliament; and

**(b)** the data is in the possession or control of the institution, person or entity and will assist in the investigation of the offence.

Complementary and similar authorities (and conditions on using them) are included in sections 487.015 (production order to trace specified communication), 487.016 (production order – transmission data) and 487.018 (production order for financial information).

Generally speaking the production orders are the main tools used by police when they are seeking customer records and data. However, production orders are only used on cooperative third parties and in the circumstance where police have an uncooperative third party they can still avail themselves of the section 487 search warrant to physically seize customer records and data themselves.

For a full description of the offences see the current text of *Criminal Code* available at <http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html>.

***Canadian Security Intelligence Service Act* (CSISA)**

Other relevant rules are included in the CSISA which contain provisions authorizing interception of communications to enable the Canadian Security Intelligence Service to investigate a threat to the security of Canada and to perform certain other statutory duties or functions. Such interceptions (which may involve the capturing of customers data) must be authorized by a warrant issued by a judge pursuant to the CSISA. An application for such warrant must be approved in advance by the Minister of Public Safety and Emergency Preparedness (see full text at <http://laws-lois.justice.gc.ca/eng/acts/c-23/>).

***Convention on Cybercrime***

In this context, is it also noteworthy that in 2015 Canada has ratified the Council of Europe's *Convention on Cybercrime*, an international treaty that provides signatory states with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence.

**2. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to (a) suspend or restrict access to websites and telecommunications networks and the requests to provide or (b) facilitate access to customer data;**

***Privacy Act* (PA)**

The PA imposes obligations on federal government departments and agencies with respect to the collection, use and disclosure of personal information that they handle. The PA has been recognized as having a quasi-constitutional status. As the PA requires that a federal agency have Parliamentary authority before it engages in the collection of personal information from a telecommunication provider, any specific legislation authorizing law enforcement agencies to collect customer information held by telecommunication companies (more specifically the *Protecting Canadians from Online Crime Act*) is applicable in conjunction with the PA.

***Personal Information Protection and Electronic Documents Act* (PIPEDA)**

As a general rule, the PIPEDA requires that organizations keep personal information (including customers data) confidential, and provides that organizations may only collect, use or disclose personal information with the knowledge and consent of the person to whom the information relates. Section 7 of PIPEDA contains several exceptions to this general rule and permits organizations to collect, use and disclose personal information without consent albeit in limited and defined circumstances. While those exceptions permit organizations to disclose personal information without consent, they do not give government institutions the right to access or obtain that information.

**Transparency reports**

Non-binding Transparency Reporting Guidelines has been published on June 30, 2015 (see <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html>). They aim at helping private organizations being open with their customers regarding the management and sharing of their personal information with government entities such as law enforcement and national security agencies.

It may be worth adding that the Minister of Public Safety and Emergency Preparedness of Canada is obligated under section 195 of the *Criminal Code* to produce and present to the Parliament annual reports that detail the regularity with which they intercept Canadians’ communications, including customer data.

The most recent report, for 2014, is available here: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2014/index-en.aspx>

**3. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points;**

A number of statutes govern the activities of private entities that provide network components or related technical support.

***Telecommunications Act***

The TA applies to Canadian Carriers and, to certain extent regarding the conditions of services (see s. 24.1 of the TA) to any person other than Canadian carrier (including a provider of network component or related technical support).

The TA specifically requires from Canadian carriers not to impose rates for telecommunications services that are unjust or unreasonable and specifically that unduly discriminate or give an undue or unreasonable preference in relation to the provision of a telecommunications service (TA, s. 27 (1)-(2)).

Accordingly, the TA requires Canadian carriers to provide telecommunications services and charge rates that are just and reasonable and not unduly discriminatory, in accordance with any orders made under section 8 of the TA (which authorizes Governor in Council to issue direction to the CRTC) and any technical standards prescribed by the Minister of Industry under section 15 of the TA (TA, s. 47).

The TA also regulates submarine cable providers. Its section 17 prohibits any person from constructing or operating an international submarine cable “except in accordance with an international submarine cable licence”. The licence can be obtained on application to the Minister of Industry and may be subject to such conditions “as the Minister considers are consistent with the Canadian telecommunications policy objectives” specified in section 7 of the TA (TA, s.19(2)). The terms of the licence cannot exceed ten years but may be renewed for another ten years (TA, section 19(3)).

Section 34(1) of the TA confers on the CRTC a power to forbear from exercising certain powers (relating to performance of any duty under sections 24, 25, 27, 29 or 31 of the TA) in relation to a telecommunications service or class of services provided by a Canadian carrier. However, the CRTC has retained (in part) its powers under section 24 of the TA so that, among other things, it may impose conditions on the offering and provision of retail Internet services as may be necessary in the future. Those powers may be used by the CRTC to order a Canadian carrier to cease providing service when a condition of service, adopted pursuant to section 24 of the TA and which applies to that carrier, is not satisfied.

Furthermore, as stated above, section 36 of the TA prohibits a Canadian carrier from controlling the content or influencing the meaning or purpose of telecommunications carried by it for the public, unless the CRTC approves otherwise.

Today virtually all voice and data communications markets in Canada are open to competition and, generally speaking, the CRTC has chosen to a large extent not to regulate the Internet.

***Radiocommunication Act* (RA)**

The RA prohibits any person from installing, operating or possessing radio apparatus except in accordance with radio authorization issued by the Minister of Industry pursuant to the RA unless exclusion applies (RA, section 4(1)). Microwave transmission facilities, wireline and cellular telephones, satellites, and satellite earth stations are among the types of telecommunications apparatus that require an authorization pursuant to this provision, and private entities that provide these services are subject to it.

**Canada’s Anti-spam Legislation and Regulations**

Under CASL private entities, such as those that provide network components or related technical support are not allowed to send commercial electronic messages without the prior consent of the recipient (CASL, section 6), alter transmission data (CASL, section 7), or install computer programs without proper authorization (CASL, section 8). Under section 9 of the CASLA it is also prohibited to aid, induce, procure or cause to be procured the doing of any act contrary to any of sections 6 to 8. A number of exemptions in CASL and the *Electronic Commerce Protection Regulations*, SOR/DORS 81000-2-175, limit the scope of those prohibitions.

**Other Acts**

In addition Canada also enacted legislation pertaining to certain carriers, including *Bell Canada Act*, the *Teleglobe Canada Reorganization and Divestiture Act* and the *Telesat Canada Reorganization and Divestiture Act*.

**4. Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data;**

**Remedies under *Canadian Charter of Rights and Freedoms* (Charter)**

In the event of undue restrictions on Internet and telecommunications access or undue access to customer data, all Canadians benefit from the constitutional guarantees inscribed in the *Canadian Charter of Rights and Freedoms* and can seek, for example, a court order to protect their rights. The Charter, which is part of the Constitution of Canada, provides for the protection of freedom of expression (under section 2(b)) as well as the right to be secure against unreasonable search or seizure (under section 8) among other rights and freedoms.

Canadian courts have interpreted both provisions very broadly. If a court concludes that a Charter provision has been violated, the government has the burden to establish that the limit to the right or freedom is justified under s. 1 of the *Charter*, which guarantees the rights and freedoms set out in it subject “only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society”. In the event of an unjustified violation of a Charter right, s. 24 of the Charterallows a court of competent jurisdiction to grant any remedy that it considers “appropriate and just in the circumstances,” including for example awards of damages, and may declare that laws are of no force and effect.

Expression protected by s. 2(b) has been defined as “any activity or communication that conveys or attempts to convey meaning” (*Thomson Newspapers Co. v. Canada (Attorney General)*, [1998] 1 S.C.R. 877). The courts have applied the principle of content neutrality in defining the scope of s. 2(b), such that the content of expression, no matter how offensive, unpopular or disturbing, cannot deprive it of s. 2(b) protection. Rather, the content of expression can be examined in determining whether a restriction is justified under s. 1 of the *Charter*.

The Supreme Court of Canada has also made several recent pronouncements concerning the principles that govern search and seizure of communications data and communications devices by law enforcement authorities in the context of the constitutional protection against against unreasonable search or seizure under section 8 of the Charter. For example, in *R. v. TELUS Communications Co.* [2013 SCC 16] the Court confirmed that text messages will be protected in a similar manner to voice conversations. In its more recent decision in *R. v. Spencer* [2014 SCC 43], the issue was whether police action to obtain information associated with the defendant’s IP address constituted an unconstitutional search.  The Court held that the police request for the subscriber information constitutes a “search” and that subscriber information corresponding to internet activity engages a high level of informational privacy. In the absence of lawful authority, the search was illegal and infringed the defendant’s rights protected under section 8 of the Charter.

**Reviews of CRTCs decisions under the *Telecommunications Act***

Section 62 the TA provides the CRTC with the power to reconsider its own decision. It may, on application or on its own motion, review and rescind or vary any decision made by it or re-hear a matter before rendering a decision. In Telecom Information Bulletin [2011-214](http://www.crtc.gc.ca/eng/archive/2011/2011-214.htm), the CRTC outlined the criteria it would use to assess review and vary applications filed pursuant to section 62 of the TA. Specifically, the CRTC stated that applicants must demonstrate that there is substantial doubt as to the correctness of the original decision, for example due to:

* + an error in law or in fact;
	+ a fundamental change in circumstances or facts since the decision;
	+ a failure to consider a basic principle which had been raised in the original proceeding; or
	+ a new principle which has arisen as a result of the decision.

As a general rule of law, public officials or agencies must follow proper procedures to arrive at their decisions. Virtually all judicial supervision of federal administrative actions is assigned to the Federal Court of Canada. CRTC decisions on questions of law or jurisdiction can be subject to appeal in Federal Court of Appeal (with leave of that court pursuant to section 64(1)). The appeal must be brought within 60 days after the day on which leave to appeal is granted (TA, section 64(1)(4)).

An alternative venue to challenge a CRTC decision is provided in Section 12 of the TA. Any decision of the CRTC can be varied, rescinded or referred back to the CRTC for reconsideration by an order of the Governor in Council (GiC) on its own motion or on petition within one year of its date. In exercising the powers vested in it under section 12, the GiC may act (or decide not to act) either on its own motion, or in response to a petition. Based on this provision there are only a few easy to meet statutory preconditions for a valid petition. The latter must be in writing, with regards to a valid, subsisting decision of the CRTC, and presented to GiC within 90 days after the CRTC decision. The GiC often makes decisions with regards to petitions based on broader policy considerations on matters of public interest.

**5. Other relevant laws, policies or initiatives to promote or enhance Internet accessibility and connectivity, including measures to promote network neutrality.**

The *Telecommunications Act* (in s. 7(b)) affirms that the Canadian telecommunications policy has among its objectives “to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada” (the “universal service objective”).  The TA requires from Canadian carriers not to impose rates for telecommunications services that are unjust or unreasonable and unduly discriminate or give an undue or unreasonable preference in relation to the provision of a telecommunications service. (TA, s. 27 (1)-(2). The act empowers the CRTC to ensure compliance with these and other obligations and confers broad regulatory powers on the CRTC for that purpose. Moreover, as stated above, section 36 of the Act promotes the net neutrality by prohibiting controlling the content or influencing the meaning or purpose of telecommunications carried by Canadian carriers for the public (unless the CRTC approves otherwise).

In Telecom Decision CRTC 99-16, the CRTC made the universal availability of telephone service at affordable prices, as endorsed by the TA, one of its prime objectives. This includes providing universal availability of low speed data transmission to the Internet at local rates. While CRTC also contemplated adding access to broadband Internet services, it concluded that it lacks legal authority to do so (see <http://www.crtc.gc.ca/eng/archive/1999/dt99-16.htm>). In 2011 the CRTC has conducted a comprehensive review of the issues surrounding the duty to serve and the obligations telecommunications carriers bear, or should bear to address the issues of providing telecommunication services and decided that it will not require broadband Internet access to be provided as part of any basic service objective (Telecom Regulatory Policy CRTC 2011-291, see <http://www.crtc.gc.ca/eng/archive/2011/2011-291.htm>). The Commission is currently in the process of reviewing the scope of the obligation to serve and the basic service objective (Telecom Notice of Consultation CRTC 2015-134, see <http://www.crtc.gc.ca/eng/archive/2015/2015-134.htm>) and has initiated public proceedings to examine differential pricing practices used by Canadian Internet service providers in their wireless and wireline plans (Telecom Notice of Consultation CRTC 2016-192, see <http://www.crtc.gc.ca/eng/archive/2016/2016-192.htm>).

In addition, some measures have been undertaken to ensure the availability, reliability, efficiency and optimal use of the telecommunications networks as well as ensuring the privacy of Canadians is not compromised. For instance, pursuant to section 41 of the TA, the CRTC may, by order, prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the CRTC considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression. The CRTC maintains a current version of the Unsolicited Telecommunications Rules on its website at <http://www.crtc.gc.ca/eng/trules-reglest.htm>.

The CRTC prohibited also the use of Automatic Dialing Announcing Devices to make unsolicited call for the purpose of solicitation (Telecom Decision CRTC 94-10).

Moreover, rules related to the protection of electronic commerce were introduced in 2010 and are included in the Canadian Anti-Spam legislation. The purpose of CASL is to promote the efficiency and adaptability of the Canadian economy, in protecting the freedom of expression, by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities, because, among other things, such conduct:

* impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities;
* compromises privacy and the security of confidential information;
* undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities in Canada and abroad.

For those reasons, as described above, CASL prohibits certain commercial practices (under ss. 6 to 9) to assure better connectivity for Canadians.