Answers to the questionnaire on "La responsabilité secondaire des prestataires de services/Secondary Liability of Service Providers"

Pierre TRUDEL, Professor
Director, *Centre d'études sur les médias*
Holder of the L.R. Wilson Chair in Information Technology and E-Commerce Law
Centre de recherche en droit public, Faculty of Law
Université de Montréal
P.O. Box 6128, Postal Station "Centre-ville"
Montréal, QC, Canada H3C 3J7
Tel: (514) 343-6263 - Fax: (514)343-7508
www.chairelrwilson.net

In Canada, civil liability law is in principle under the jurisdiction of the provincial parliaments. General civil liability law varies from province to province, but Québec law is special with respect to liability issues because, unlike the other provinces where there are common law regimes, its sources are in French law. The present report describes the situation in Canadian law, but uniquely with respect to the law of the Province of Québec.

I. Secondary Liability Standards

1. What are the elements required to establish secondary (or indirect, or accessorial) liability of service providers for the conduct of others using their services? Is there more than one basis on which to establish secondary liability? (For example, in some countries, contributory liability may co-exist with vicarious liability.)

In Québec, the principle set out in Section 22 of the *Act to Establish a Legal Framework for Information Technology* is that a service provider is not responsible for the activities of people using its services through documents stored by the user or at the user's request. The Section is as follows:

> A service provider, acting as an intermediary, that provides document storage services on a communication network is not responsible for the activities engaged in by a service user with the use of documents stored by the service user or at the service user's request.
>
> However, the service provider may incur responsibility, particularly if, upon becoming aware that the documents are being used for an illicit activity, or of circumstances that make such a use apparent, the service provider does not act promptly to block access to the documents or otherwise prevent the pursuit of the activity.
>
> Similarly, an intermediary that provides technology-based documentary referral services, such as an index, hyperlinks, directories or search tools, is not responsible for activities engaged in by a user of such services. However, the service provider may incur responsibility, particularly if, upon becoming aware that the services are being used for an illicit activity, the service provider does not act promptly to cease providing services to the persons known by the service provider to be engaging in such an activity.

Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.

Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.

This exoneration of responsibility holds until the service provider has *de facto* knowledge of the illicit nature and if it does not take prompt action to block access to the documents or otherwise prevent the activity from continuing. The provision establishes the non-liability of such service providers, but the limitation on liability ceases to have effect if certain facts are established. Once such facts are established, there is a possibility that the intermediary's liability will be incurred. Thus the liability is indeed secondary since so long as the condition of knowledge is not met, the intermediary has no liability.

The elements required for liability to be incurred are knowledge of the illicit nature or of circumstances making it apparent.

When they gain knowledge of the illicit nature of an activity associated with documents that they store or to which they provide access, hosting and search engine service providers are obliged to take action. The factor that triggers their liability is the knowledge they have or acquire of the illicit nature of the information. However, this is not the only situation in which the liability of these intermediaries can be incurred. Section 22 does not contain an exhaustive list of situations in which an intermediary that is targeted can incur liability. The second paragraph of Section 22 says that a provider "may incur responsibility, particularly if, upon becoming aware..." The same formulation is repeated in the third paragraph concerning providers offering search tools.[1]

---

1 See: Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, (Cowansville: Éditions Yvon Blais, 2012), c. 7; Pierre TRUDEL, "La responsabilité des acteurs du commerce électronique," in Vincent GAUTRAIS, Ed., *Droit du commerce électronique*, (Montréal: Éditions Thémis, 2002), p. 607-649; Pierre TRUDEL, "Les responsabilités dans le cyberspace," in *Les dimensions internationales du droit du cyberespace, collection Droit du cyberespace*, (Paris: Éditions UNESCO - Economica, 2000), 235-269; Pierre TRUDEL, "La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information," in FORMATION PERMANENTE, BARREAU DU QUÉBEC, *Développements récents en droit de l'Internet*, No. 160, (Cowansville: Éditions Yvon Blais, 2001), p. 107-141.

A. The "illicit" nature

Section 22 specifies that the liability that may flow from documents put online by others concerns illicit statements, documents and activities.

In the French *Larousse* dictionary, "*illicite*" is defined as "what is forbidden by morals or the law." [Our translation.] Jean Deliyannis considers as illicit "Any action contrary to the very principles of the law, namely, any unjust or simply antisocial action […] even if it is not formally prohibited by law."[2] However, this author adds that, as an element of misconduct (in the legal sense), we cannot give the notion of illicit such scope that it would cover even actions that do not give rise to disapproval.[3]

The notion of disapproval has to be assessed in an environment in which freedom of expression plays an important role. In democratic societies, freedom of expression protects even statements that can give rise to disapproval. This is why we come back to the criterion of statements that are against the law. Since in Canada it is the law and only the law that can set limits on freedom of expression, we have to base ourselves on the law to determine whether a statement, piece of information or activity is illicit in the sense of Section 22.

B. *De facto* knowledge

The liability of intermediaries targeted by Section 22 can be incurred if it is established that they had *de facto* knowledge of the illicit nature of activities performed by the service user by means of technology-based documents.

Owing to the rule set out in Section 26, which excludes the obligation to conduct active monitoring, we cannot deduce intermediary misconduct from failure to conduct surveillance. Consequently, it is hard to see how an intermediary could be considered as having knowledge of the content of documents from the simple fact that they pass through its hands. It acquires knowledge only when it is notified that there is an activity that is illicit in nature or of circumstances that make an illicit activity apparent.

Knowledge can be ascribed in a number of circumstances. First, it is presumed as soon as the information is produced by the person himself or herself, or the person has made the decision to publish it. Thus, if a hosting service provider stores documents that originate with it, it will obviously be considered to have knowledge of the content of those documents.

If the intermediary plays an active role with respect to the documents or activities, knowledge about the stored documents can be presumed. For example, in *L'Oréal SA and Others* v. *eBay International AG and Others,*[4] the European Union Court of Justice found that eBay can claim this status and the ensuing

---

2 Jean DELIYANNIS, *La notion d'acte illicite, considéré en sa qualité d'élément de la faute délictuelle*, (Paris: Librairie générale de droit et de jurisprudence, 1952), p. 328. [Our translation.]

3 *Id.*, p. 329.

4 Judgment of the Court (Grand Chamber) of 12 July 2011. *L'Oréal SA and Others* v. *eBay International AG and Others*. < http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3205 >. See: "eBay hébergeur sous conditions, selon la CJUE," *Legalis.net*, 13 July 2011, < http://www.legalis.net/spip.php?page=breves-article&id_article=3206 >.

exoneration of liability if it has not played an active role that would give it knowledge of or control over the data stored.

Second, a person may have *de facto* knowledge if he or she conducts constant or occasional monitoring of a site or environment. There is no obligation to conduct surveillance in order to acquire knowledge as soon as illicit documents appear, but if such monitoring is done and it makes it possible to acquire knowledge of the illicit nature of documents, then the service provider's liability can be incurred if it does not take action.

Third, knowledge can be acquired through notification by a third party. This is the situation in which a person brings to the attention of the storage service provider the fact that it is storing illicit documents.

Finally, when the illicit nature of a targeted document is controversial, the service provider's liability is incurred only from the time when the illicit nature has indeed been established.

C. Knowledge of circumstances making an illicit activity apparent

Knowledge can concern circumstances that make an illicit activity apparent. Such knowledge can flow from indications that come to the service provider's attention and lead to the conclusion that there is illicit activity.

However, the provider of such services often has no legitimate reason to intervene in order to eliminate potentially harmful information. Aside from absolutely clear cases of illicit activity, in the name of what and in virtue of what authority would the service provider have to judge the illicit, or permissible, nature of a given piece of information? In virtue of what authority should it play the role of a judge responsible for determining whether content is harmful or damaging?

D. The degree of knowledge required to incur liability

Points of view may differ as to the degree of knowledge necessary to incur the liability of a service provider. Strowel and Ide note that "the whole question is how to define the threshold of knowledge for full liability to come into play."[5] Given the imperatives of freedom of expression, the threshold of knowledge for the intermediary's liability to be incurred has to be more than a mere complaint or allegation. For a person to be justified in taking action with respect to a piece of content, that person has to have acquired confirmed knowledge of the indeed illicit nature of the document. The knowledge that unleashes liability is not that which results from simple reception of a complaint, but rather that acquired at the point when the illicit nature becomes manifest. This is what makes it possible to say that when the illicit nature is apparent on the very surface, knowledge of it is acquired as soon as the existence of the document is known.

In clear cases, if there are any, there is an easy answer to the question: if the illicit nature is blindingly obvious, the intermediary may have a duty to take action as soon as a complaint is received. However, what is to be done in situations where the illicit nature is not obvious? For example, what if a hosting service provider receives notification to the effect that a given document that it is hosting contains

---

5 Alain STROWEL and Nicolas IDE, "Responsabilités des intermédiaires: actualités législatives et jurisprudentielles," in *Droit Nouvelles technologies*, < http://www.droit-technologie.org/dossier-26/responsabilite-des-intermediaires-actualites-legislatives-et-jurispru.html >. [Our translation.]

information that violates a person's image rights? We know that there are many situations in which publishing a person's image is perfectly licit. If the service provider complies with the request and removes the document, it is acting as a judge, but as a judge who has taken action without fulfilling the elementary obligation to hear the arguments of all the parties involved in the case. If the intermediary does nothing, it exposes itself to incurring liability and having to defend itself if the victim takes legal action. If it takes action and removes the information, it exposes itself to charges by the publisher of the information hosted or linked that it did not take elementary precautions to ensure that the notification was well-founded. This dilemma has led American and French legislators to introduce a procedure designed to separate serious allegations from whims.

Since the Québec legislator has not said anything specific about what should be done in this respect, should we conclude that there are no obligations concerning the precautions to be taken following reception of notification to the effect that a hosted or linked site is illicit? The answer to this question has to be no. Hosting and search engine service providers can incur liability if they comply with a notification without taking minimum precautions. A person whose documents are removed from a site or banned from an indexing system could certainly suffer damages from an unfounded allegation that the documents are illicit. The problem then arises of how to determine whether the intermediary has acted in a prudent manner and taken the precautions that a reasonable person should have taken under such circumstances. If the notification proves frivolous or poorly founded, the service provider will have removed content, violated freedom of expression and promoted the desires or even the whims of a complainant instead of prudently applying a measure that constitutes censure, and is thus an essentially exceptional action. Gingras and Vermeys rightly note that the intermediary is not required by contract to link or even, in some cases, to host.[6] However, this does not prevent it from being taken for granted that such intermediaries have a duty to employ prudence when they remove documents from their environments.

What is at stake here is thus how to establish that an intermediary has had a reasonable attitude. It is not up to the service provider to make a decision on its own about whether material targeted by a notification is indeed illicit, but rather to determine whether a reasonable person might consider that the material is or is not illicit.

In such a situation, the appropriate attitude for the intermediary is to obtain confirmation from a third party, such as a neutral expert, and to act on the basis of that evaluation. Indeed, *de facto* knowledge begins only when a complaint is sufficiently documented to remove all reasonable doubt as to its seriousness. This approach is compatible with a conception that respects freedom of expression and the public's right to information. It is difficult to see in virtue of what principle we should always assume a complaint about a document is valid without taking at least the precaution of verifying whether a reasonable person would consider the document illicit. Censure would then occur without any serious examination of the claims that the document is illicit. It would be astonishing if the Québec legislator had opted for a practice so inconsistent with the principles of democratic society.

Consequently, so long as the intermediary has not received independent confirmation of the illicit nature of a document, it has no obligation to act in a manner that censures the information. If it does so, it exposes itself to the possibility of having wronged the publisher of the document. Thus, the intermediary

6 P. GINGRAS and N. VERMEYS, *Actes illicites sur Internet : qui et comment poursuivre?*, (Cowansville: Éditions Yvon Blais, 2011), p. 39.

does not have knowledge of the illicit nature of the information or document until it is able to establish the seriousness of the complaint or notification. It is only from that point that it has the obligation to take prompt action.

Reasoning otherwise would amount to giving anyone who thinks he or she has been harmed by a document the power to perform prior censure without the intervention of a third party able to weigh claims. There is a right to remove information once its illicit nature is established, but it would be absurd for a legislator to institute legislation allowing anyone to obtain, through a simple complaint, removal of information that he or she dislikes or considers damaging. The target of the *Act*'s provisions is illicit information. For a complaint to be serious, it has to show serious reasons leading to the conclusion that the targeted document is illicit, and not flow from an arbitrary, revengeful or frivolous claim. In order to draw the conclusion that a complaint is serious, an intermediary with doubts in that respect would be wise to obtain independent confirmation.

When an intermediary asks whether a document in its environment is illicit, the purpose of the independent confirmation is not to determine whether the document is indeed illicit, but rather whether it is reasonably possible that an appropriately informed court would come to the conclusion that the document targeted by the notification is illicit. In sum, the legal professional does not decide whether or not the document is illicit: he or she assesses whether the document could be considered illicit by a reasonable person who, appropriately informed, evaluates it. Thus, the evaluation would in particular have to determine what law the document might violate. Such a solution avoids an approach involving prior censure of documents expressing critical points of view, such as that adopted in the story reported on the JE program on October 23, 2009 concerning the "monavis.ca" site.[7] In that case, the intermediary found no better strategy than to remove critical comments without investigating whether they did indeed violate a law.

It seems that the intermediary's liability can flow only from real knowledge of the illicit nature of a document. Reasoning otherwise would amount to giving all complainants a right to prior censure, which would violate freedom of expression.

E. The obligation to promptly cease providing services to persons known to be engaged in illicit activities

The obligation to promptly cease providing services to persons known to be engaged in illicit activities is incumbent on the service provider when knowledge of the illicit nature has been established. If they perform the mentioned actions once they have acquired knowledge of the illicit nature of the documents or activities, the service providers targeted in Section 22 have no liability.

As soon as it acquires knowledge of the fact that persons are engaged in an illicit activity, a search engine service provider has the obligation to take prompt action to cease providing services. A hosting service provider must block access to the documents or prevent the illicit activity from continuing. The means that must be employed to fulfill the obligation to take prompt action are assessed in accordance with the service provider's circumstances.

---

7 TVA, Émission JE, *Diffamation sur Internet*, < http://tva.canoe.ca/emissions/je/reportages/61586.html > visited on February 23, 2012.

The service provider must take action in a prompt manner, rapidly. The obligation to take action arises with the knowledge; it begins as soon as the illicit nature is established in a serious, independent manner. Evaluation of whether or not the service provider has taken prompt action will be based on when it acquired knowledge of the illicit nature. Whether the promptness was sufficient is based on the circumstances, the means required and the effort made to take action.

The service provider's action has to make access to the documents impossible or otherwise prevent the activity from continuing. It must employ the means possible, given the resources available and the circumstances. The service provider has no liability if the actions necessary to correct the situation are performed promptly.

F. Exclusion of the obligation to engage in active monitoring

The rules concerning liability on the Internet belong to the realm of general law. The principles of civil liability law are applicable, but the legislator has added certain conditions so that the liability of the targeted service provider is incurred.[8] Once it is incurred, the civil liability of an intermediary, like that of any other person, necessarily flows from a misdeed on its part. Once it has been established that it knew of the illicit nature of a document or activity, the intermediary service provider's liability may be incurred. However, it will then be necessary to show that the intermediary behaved in a manner inconsistent with that of a prudent, diligent person placed in similar circumstances.[9]

In line with the European directive,[10] Section 27 of the *Act* provides that intermediaries have no obligation to engage in active monitoring. Section 27 is as follows:

> 27. A service provider, acting as an intermediary, that provides communication network services or who stores or transmits technology-based documents on a communication network is not required to monitor the information communicated on the network or contained in the documents or to identify circumstances indicating that the documents are used for illicit activities.

---

8 Cyril ROJINSKY, "Commerce électronique et responsabilité des acteurs de l'Internet en Europe," < http://www.droit-technologie.org/dossier-21/ > (site visited on February 27, 2012).

9 Jean-Louis-BAUDOUIN and Patrice DESLAURIERS, *La responsabilité civile*, 5th Edition, (Cowansville: Éditions Yvon Blais, 1998), No. 154; Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF and Sophie HEIN, *Droit du cyberespace*, (Montréal: Éditions Thémis, 1997), 1296 p., c. 5.

10 Article 15 of the *Directive on electronic commerce* reads as follows : "1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

> However, the service provider may not take measures to prevent the person responsible for access to documents from exercising his or her functions, in particular as regards confidentiality, or to prevent the competent authorities from exercising their functions, in accordance with the applicable legislative provisions, as regards public security or the prevention, detection, proof and prosecution of offences.

Section 27 specifies the obligations incumbent on a service provider "acting as an intermediary, that provides communication network services" or stores or carries technology-based documents. A number of intermediaries are targeted by this provision: hosting, archiving and carrying service providers, but also any other intermediary that provides services on a communication network or that stores or carries technology-based documents.

Sections 22, 36 and 37 of the *Act* state the general legal regime for companies doing business in the province. They set out what constitutes, for the intermediaries targeted, appropriate behaviour. However, even if they perform actions that deprive them of the provided-for immunity, intermediaries are not automatically liable. The legislation is careful to provide that their liability "may" be incurred if they have not adopted an attitude that gives them access to the immunity provided for under the legislation. If this is the case, their actions and omissions will be examined in accordance with the general legal criteria for civil liability.

Section 27 says that intermediaries have no obligation to engage in active monitoring. It is thus not a fault on their part if they have not done active monitoring. Such service providers are not required to monitor information or watch for circumstances that could indicate that documents are being used for illicit activities. However, such intermediaries must not take any action to prevent the person responsible for access to documents from performing his or her duties in compliance with the law, in particular with respect to confidentiality. They must also not take action to prevent the competent authorities from performing their duties in accordance with the law in relation to public security and crime prevention, detection, proof and prosecution. The actions of authorities responsible for public security and crime prevention are limited by the legislation that provides the framework for the work of such authorities.

The exclusion of the obligation to engage in active monitoring is accompanied by a prohibition against interfering with the person responsible for access to documents in cases in which the environment in question falls under an access to documents regime. It is also prohibited to prevent the competent authorities from performing their duties with respect to public security and the prevention, detection, proof and prosecution of offences. However, as soon as an intermediary begins to play an active role, it loses the advantage of not being obliged to conduct monitoring, for example, by becoming involved in access to documents or by intervening between the forces of order and documents.

Nonetheless, exclusion from the obligation to engage in active monitoring has its limits. Apparently, it comes to an end when content that is indeed illicit has been brought to the intermediary's attention. According to a Paris *Tribunal de commerce* (Commercial Court) decision, as soon as a copyright holder has given notice of illicit content in a hosting service provider's storage system, the hosting service provider is obliged to monitor for any new appearance of that content, anywhere documents are stored on its site.[11]

---

11 *Flach Film et autres v. Google France, Google Inc.*, Tribunal de commerce de Paris, 8e chambre, Jugement du 20 février 2008, Legalis.net, < http://www.legalis.net/breves-article.php3?id_article=2223 > (site visited on February 27, 2012).

2. Do the laws creating such possible liability consist of a single horizontal standard applicable without regard to the specific area of law in question, or does the liability standard vary according to the cause of action (e.g., intellectual property, defamation, etc)?

Sections 22, 26, 27, 36 and 37 of the *Act* apply to all areas under Québec's jurisdiction. They establish a conditional regime of exoneration of liability in favour of certain technology-based intermediaries. Consequently, service providers involved in transmitting documents are, if they comply with certain conditions, exonerated of liability for the documents transmitted.

The limited liability regime applying to these intermediaries concerns areas under the jurisdiction of the Parliament of Québec. The *Act* explicitly excludes certain obligations from applying to such intermediaries in order to delimit the scope of behaviour that can be considered as incurring their liability.[12]

3. Do laws creating the secondary liability of service providers for conduct of others using their services define (or make use of) the concept of a "service provider"? Is the definition limited to internet (or online) service providers? Please provide example of service providers falling within any such definition. Does the definition encompass search engines and operators of online market places?

The *Act* targets entities that perform intermediary functions. The limits on liability provided for in the *Act* are not based on types of operators or intermediaries: they focus on the type of activity performed, for example, carrying, indexing and hosting. Consequently, when intermediary liability is examined, the way entities are designated should not be considered important, but what they do or should have done with respect to an illicit document or piece of information. The *Act* establishes rules applying to any service provider that finds itself in the described situation and that does or does not do the actions mentioned in the legislation.

The *Act* states the rules applying to any service provider that is indeed in the described situation and that does or does not perform the actions mentioned in the *Act.* Such service providers are:

- Service providers offering to store technology-based documents on a communication network. The archetype is a hosting service provider, but the notion is broad enough to encompass all service providers who receive documents that they store and make available on the network. For example, user-generated content environments fit this description.
- Service providers offering links to technology-based documents, including indexes, hyperlinks, directories and search tools.
- Service providers offering communication network services exclusively for the transmission of technology-based documents. We shall call this type of intermediary a "carrier."

12 Concerning criminal liability, see: Sevgi KELCI, *La responsabilité pénale des intermédaires techniques, à la lumière des pratiques internationales*, (Cowansville: Éditions Yvon Blais, 2010).

- Intermediaries that store documents for the sole purpose of ensuring efficient transmission. This category targets service providers that act as intermediaries, and store on a communication network technology-based documents provided by clients only to ensure the efficiency of later transmission to persons who have the right to access the information.

4. Were the standards for establishing secondary liability of service providers for the conduct of others using their services first developed by the courts or created by statute? If developed by the courts, from which existing principles (if any) did the courts draw?

The responsibility standards for establishing the secondary liability of service providers targeted by the *Act* flow essentially from the legislation.

5. To what extent does the standard for secondary liability discussed in answering the previous question depart from the general standard for establishing secondary liability in tort (or other relevant) law?

The legislation introduces a condition that must be met for the targeted intermediaries to incur liability. If the condition is met, the general law on liability applies.

6. What is the relationship between the standard for secondary liability of service providers and the relevant standard for primary liability (either of the service providers or third parties using their services)? To what extent have courts assessing the scope of primary liability taken into account the possibility of secondary liability of service providers (and vice-versa)? To what extent is secondary liability tied to establishing primary liability of others?

So far, Québec courts have not had to rule on these issues.

7. What remedies will a court grant where a service provider is found secondarily liable for the conduct of others? Do these remedies differ from those available against the third parties who are primarily or directly liable? In determining remedies, do courts take account of relief available against those who may be directly or primarily liable?

So far, Québec courts have not had to rule on these issues.

II. Immunity from Secondary Liability

1. Are there laws immunizing (or providing a so-called "safe harbor" for) service providers against liability for conduct of others using their services?

Section 22 of the *Act to Establish a Legal Framework for Information Technology* creates a zone in which targeted service providers are immune. They have no liability if and as long as they have no knowledge of the illicit nature of a document or activity carried out using technology-based documents. As soon as they acquire such knowledge, maintenance of their immunity is conditional on them taking prompt action to make the illicit document unavailable.

2. If so, what is the definition of a "service provider" for this purpose? Is the immunity conferred limited to internet (or online) service providers?

The service providers targeted by this immunity are those who act as intermediaries to offer technology-based document storage services on a communication network. Service providers who act as intermediaries to provide links to technology-based documents, including indexes, hyperlinks, directories and search tools, also enjoy this immunity.

3. If immunity is available, is it conferred against liability without regard to the specific area of law in question?

The immunity is conferred with respect to all areas concerning civil and criminal liability in accordance with the laws of Québec.

4. Against what forms of liability (e.g., only secondary liability, only damages) is immunity offered? What conditions must a service provider satisfy to take advantage of immunity?

When immunity applies, it concerns all of the service provider's liability. The service provider enjoys the immunity on the condition that it does not know of the illicit nature of the document put online by a cybernaut.

5. Was the provision of law conferring immunity developed by courts or created by statute? If developed by the courts, from which existing principles (if any) did the courts draw?

This immunity has been conferred by statute.

6. Does the law in your country provide for the possibility of remedies being awarded against service providers to help restrain wrongful conduct by others independent of the service providers being secondarily liable? If so, in which circumstances will courts grant such remedies, and for what purpose?

The legislation does not provide for this.

7. If your answer to Question 6 is in the affirmative, what types of remedies will courts consider when the service providers are not secondarily liable(e.g., information disclosure, or DNS and IP address blocking). How do these remedies differ from those imposed in the event of secondary liability being established?

Not applicable.

III. Other Questions

1. To what extent have service providers developed best practices or voluntary codes for dealing with conduct by third parties using their services that allegedly amounts to a violation of law?

2. **If your answer to Question 1 is in the affirmative, who was involved in the development of such practices or codes? In what form have these been embodied (e.g., a memorandum of understanding with select right holders, or a settlement agreement)? Have courts paid any attention to these practices or codes in deciding questions of secondary liability?**

3. **To what extent have service providers been subjected to regulatory regimes (e.g., in the online context, so-called "graduated response" systems) that require them to cooperate in the enforcement of measures against the third parties who use their service for improper purposes?**

4. **To the extent that the laws referred to above include a so-called "notice and takedown" system, has there been any concern expressed about right-holders abusing the mechanism or service providers being cautiously "over-compliant" with takedown requests? Does your law contain any penalty or disincentive for either such conduct?**

5. **What doctrinal or other mechanisms have courts used to balance the need to ensure effective enforcement of rights (or prevent unlawful conduct) with the ability of service providers to conduct business?**

6. **To what extent have fundamental or constitutional rights of service providers or their customers influenced courts' attitudes to secondary liability of the providers (or the award of remedies against the service providers in the absence of liability)?**

7. **To what extent might service providers be criminally liable for the conduct of third parties who use their services?**

8. **In disputes involving the laws discussed under Sections I and II above, to what extent have concerns about extraterritorial application of law been considered by the courts? Should they have been?**

9. **Are there any particular reforms of the current law in your country that would you believe establish a more appropriate standard for secondary liability of service providers than currently exists?**

10. **Are there any on other issues which are not covered by the questionnaire but are a concern in your country or jurisdiction?**