l'Association canadienne du droit
des technologies de l'information

January 22, 2009/22 janvier 2009

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School. Part 2 of this newsletter is prepared by Professors Pierre Trudel and France Abran of the L.R. Wilson Chair in Information Technology and Electronic Commerce Law, Université de Montréal.

Les auteurs de la première partie du présent bulletin sont les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie. Les professeurs Pierre Trudel et France Abran de le Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

Part 1

Breathalyser Law Changes Based on Advances in Technology

The issue of whether changes made to the *Criminal Code* last year limiting the types of evidence which can be called to rebut breathalyser test results arose for the British Columbia Supreme Court in *R. v. Truong*. The accused was charged with impaired driving. Subsequent to her charges being laid and only three weeks prior to her trial, amendments were made to the *Criminal Code* (see the IT.Can Newsletter of March 7, 2008). In part, those changes included a provision that the evidence challenging the accuracy of the breathalyzer reading cannot include evidence of the amount of alcohol the accused consumed; the rate at which the alcohol would have been absorbed and eliminated from the body of the accused; or a calculation based on such information as to the accused's blood alcohol concentration at the time of the alleged offence. Such an approach, referred to as a *Carter* defence, had been possible prior to the amendments, and indeed was the defence the accused had intended to lead. Subsequent to the amendments, only a defence based on proving that the equipment had malfunctioned or been improperly used was permissible.

The accused argued that the amendments were substantive, affected vested rights and therefore should be applied prospectively. In that event, she would still be able to lead her *Carter* defence, since the offence had occurred before the amendments were brought in. The Crown argued that the amendments were merely procedural or evidentiary, and therefore should operate retrospectively. The trial judge had accepted the accused's argument: on appeal the British Columbia Supreme Court concluded that this was an error and that the provision in fact did apply retrospectively. In that event the *Carter* defence was no longer available to the accused.

The appeal judge's reasoning relied on a number of factors, but in particular looked at Parliament's intention in changing the law, holding that:

> It can be seen that Parliament's intention in enacting the amendments, and the effort by Parliament to define evidence to the contrary necessary to set aside the statutory presumptions, recognizes the scientific basis of the breath test process and the reliability accorded to the approved breath testing instruments by Parliament (para 38).

The appeal judge also noted comments by the Parliamentary Secretary to the Minister of Justice regarding the purpose of the legislation. He had noted that the Supreme Court had initially, when breathalysers were introduced, allowed evidence challenging the accuracy of the results to be led, even where that evidence simply challenged whether the breathalyzer result was correct on the facts:

> Frankly, this may be a misunderstanding of what "evidence to the contrary" was intended by Parliament to be. Parliament passed the breathalyzer law in 1969, so the calculation of BAC would be done by the approved instrument, which takes the guesswork out of the equation provided the approved instrument is functioning properly, the operator uses it properly and the results are properly recorded.

> The court's interpretation may have been justified when the technology was such that operator error could affect it and there would be no direct evidence of this. Therefore, it is very much a defence that reflects the weaknesses of technology in use some 40 years ago. It was not, I believe, Parliament's intention that evidence to the contrary should be simply speculation about what an accused BAC might have been.
>
> Given today's state of technology, evidence to the contrary must be direct evidence that the machine either did not operate properly or was not operated properly. If there is no such evidence, then the BAC produced by the machine should be accepted. (para 39)

Do-not-call List

The Consumers Council of Canada has suggested that the national "do-not-call" list created by the Canadian Radio and Telecommunications Commission (CRTC) has actually resulted in an increased number of calls for some Canadians. The list was created in September of 2006, and currently has nearly six million telephone numbers registered. The CRTC has the authority to take action against telemarketers who do not fall into one of the list's exceptions and who call numbers on that list. However, the list of telephone numbers is available to anyone visiting the National Do-Not-Call website, identifying themselves as a telemarketer, and paying the appropriate fee. The Consumers Council suggests that as a result the situation with regard to telemarketing is worse than it was before. They note that if the list of numbers is used by a telemarketer located outside of Canada, the CRTC has no jurisdiction to stop those calls.

The CRTC suggests the list has been a success resulting in fewer calls for many people, and that it would take action against those misusing the list.

Evidence: Admissibility of "Nanny Cam" Master Tape

The Alberta Court of Appeal has delivered its ruling in *L.S. v. Alberta (Director of Child, Youth and Family Enhancement)*. Before the present appeal, the Provincial Court had issued an order granting the Child and Family Services (CFS) Permanent Guardianship Orders (PGO) in respect of each of the three children of the appellant. The appellant's appeal to the Court of Queen's Bench against the decision of the Provincial Court was initially struck out on technical grounds, but was re-instated by the court of appeal and heard on its merit. Even though the appeal at the Queen's Bench was based on differential standard of review, new evidence was heard on that appeal which in the opinion of the present court of appeal amounted essentially to a trial *de novo*. In that trial *de novo*, the Court of Queen's Bench sitting on appeal made adverse findings about the appellant in regard to her credibility. In dismissing the appeal, the court concluded that the appellant had engaged in sexual activity using web camera, in front of the children and that she had sexual contact with her six-year-old son and that the children had been properly apprehended under the PGO.

In the present appeal, the appellant contends, among other things, that a master tape (in which the father of one of the children recorded 160 hrs of video footage on 22 tapes using nanny cam which he secretly installed in the appellant's house) was never entered as a full exhibit during the trial. However, the appellant was cross-examined on the master tape during the appeal hearing and the appeal judge confirmed that he has started viewing the tape during lunch break. The appellant argues that it was an error for the judge to view the tape before it was admitted into evidence, and before it was identified by the person who made it or the person who edited it. She also contends that the edited version placed the events out of sequence and omitted places where she was videoed during things typical of good parenting. Generally, the appellant's contention was not that the video contained false information or was doctored to misrepresent information regarding the appellant engaging in internet sex in the presence of the children. Rather, the appellant's argument is that the judge ought not to have viewed the tape, at least at the time he did.

In rejecting this and other contentions of the appellant in regard to technological devices imported as evidence, the court held:

> In this case the proceeding was an appeal, some of which was based on an existing record, and some of which was based on admission of fresh evidence. Most importantly,

> the appeal was before a judge alone. Judges often hear or observe things over the course of proceedings that are highly prejudicial to parties and yet set aside the prejudicial material in their ultimate analysis (para 20).

The court found that the decision to admit the master tape did not disclose any error for an appellate review. Even more so, by the appeal's end the tape had been properly admitted into evidence. Given that the appellant was first to testify, it was imperative that the tape be used in her cross-examination prior to its formal admittance. More over, the appellant counsel did not object when the appeal judge indicated that he had watched the tape.

Statutory Interpretation: "Record" in Electronic Databases

The Ontario Court of Appeal has delivered its ruling in *Toronto (City) Police Services Board v. Ontario (Information and Privacy Commission)*. In this case James Rankin, a journalist with the Toronto Star newspaper, had written a series of articles in relation to the claims by the police that it does not engage in racial profiling. In order to test that claim by the Board, Rankin applied to the Board in 2003 pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (the Act) seeking information about individuals with whom the police had come into contact in course of their duties. He wanted the information to enable him to determine "whether a particular individual on record with the police, has been arrested on one occasion only or more than one occasion" (para 12). In order not to compromise the identity of the individuals implicated in the request, Rankin requested that the specific identifiers for individuals "be replaced with randomly generated, unique numbers and that only one unique number be used for each individual" (ibid). The information requested by Rankin is stored in two electronic databases (the criminal information processing system and the master name index) which the Police maintain. However, in order to process the information in the form requested by Rankin, "the Police would need to design an algorithm capable of replacing a person specific unique identifier with a randomly generated number" (para 15) and the Police have the capacity to design such algorithm using their current software.

The Police Services Board turned down Rankin's request for a number of reasons. Specifically, the Board argued that it was not legally bound to provide the record because to do so would require it to create new software that its does not *normally* use, an act outside the provisions of the Act. Rankin's appeal to the Information and Privacy Commissioner/ Ontario resulted in a finding by the Adjudicator that the information requested by Rankin constituted a record which the Police were under obligation to make available to him; even though Rankin will be required to pay the costs in regard to the form he wanted the information. In challenging the Adjudicator's finding before the Divisional Court, the Board argued that the form in which the information was requested did not constitute a record pursuant to s. 2(1)(b) of the Act, an argument accepted by the Divisional Court which upturned the order of the Adjudicator. In restoring the decision of the Adjudicator in the present appeal by Rankin, the court of appeal held that:

> Although the adjudicator did not specifically address whether the means required to produce the record *normally* used by the institution, his reasons for decision indicate that he was aware the Police would need to develop a new algorithm or software and found that the Police's concerns in this regard were addressed by the fees provisions in the Regulation enacted under the Act. In other words, he must be taken to have found that where the institution has the technical expertise, using existing software, to develop a computer program to provide a requested information, that does not take the requested information outside the s.2(1)(b) definition of record (para 41) (emphasis added).

According to the Court of Appeal, a combination of precedent, purposeful and contextual interpretation approaches to the Act suggests a more liberal construction of "record" as used in s. 2. The court found that presumptive access to information is the correct approach "because municipal institutions function to serve the public, they ought in general to be open to public scrutiny" (para 45) and the legislature's intent is to extend and improve the democratic process at the municipal and board levels so that the public could access vital information for optimal participation in that process.

2ième partie

Responsabilité de la banque lors de transfert électronique de fonds par messages

Le demandeur est un citoyen canadien d'origine gabonaise. Il poursuit la Banque de Montréal qui a accepté, sur la foi de documents falsifiés, de transférer des fonds à l'étranger par SWIFT (un système de télécommunication qui permet le transfert électronique d'argent entre différentes entités bancaires selon un message codé).

Le tribunal souligne que la banque a une obligation de moyen envers ses clients. Elle assume une obligation de prudence et de diligence. Le degré de compétence dont elle doit faire preuve comprend le respect de certaines normes liées aux usages de son commerce. À l'ère moderne de l'électronique, de l'Internet, des télécommunications sans fil et de la cyber-criminalité, les banques, institutions conservatrices, doivent faire preuve d'une adaptation qui reflète les attentes des clients. Les transactions à distance par messages génèrent un facteur de risque plutôt élevé qui fait en sorte que les banques ont une obligation de prudence et de diligence accrue. Ici, dès la première tentative par laquelle le fraudeur a voulu divertir les fonds du demandeur, une enquête aussi sommaire soit-elle sur l'authenticité de la demande aurait été nécessaire de la part de la banque. La banque a refusé cette demande de transfert mais n'aurait pas dû arrêter là, étant donné les éléments suspicieux entourant la demande. Entre autres, la demande venait de l'étranger alors que le demandeur était à Montréal et une simple vérification à l'ordinateur aurait permis de le constater. Le scénario s'est répété une deuxième et puis une troisième fois : la banque accepte des demandes de transfert de fonds sur le compte du demandeur et ce, à partir du Gabon, alors qu'une simple vérification des activités au compte aurait permis de réaliser que le demandeur était non seulement à Montréal, mais s'était même présenté à la succursale de la banque ces journées-là. Ne pas avoir procédé à ces vérifications élémentaires constitue de la négligence. La banque n'a pas exercé dans l'ensemble la prudence et la diligence dont un banquier compétent aurait raisonnablement fait preuve en l'espèce et le tribunal est d'avis qu'elle a engagé sa responsabilité contractuelle et extra-contractuelle.

- *M'Boutchou c. Banque de Montréal*, 2008 QCCS 5561 (CanLII), 21 novembre 2008.

Consultations d'offres d'emploi sur Internet

Une employée a été congédiée sans préavis par la défenderesse pour avoir consulté des offres d'emploi sur Internet durant les heures de travail. La commission des normes réclame la somme de 500$ au bénéfice de l'employée congédiée sans préavis, tel que prévu par l'article 82 de la *Loi sur les normes*. La défenderesse prétend qu'elle n'avait pas à donner un préavis car l'employée fut congédiée suite à une faute grave.

Cette notion de faute grave justifiant un congédiement sans préavis réfère à une faute d'une gravité ou d'une intensité telle qu'elle ne peut être excusée par les circonstances. Le Tribunal ne voit pas, dans le présent cas, un manque de loyauté détruisant le lien de confiance du seul fait que l'employée a consulté des offres d'emploi, ni un abus de confiance. Il souligne que l'employée « aurait-elle lu des journaux à son domicile dans lesquels des offres d'emploi étaient publiées que la défenderesse ne pourrait pas soulever la question d'utilisation de son ordinateur à des fins personnelles comme prétexte à son congédiement sans préavis. Chercher un emploi ne constitue aucunement une faute justifiant l'absence de préavis ».

- *Commission des normes du travail c. Entreprises Ernest Beaudoin Ltée*, 2008 QCCQ 12036 (CanLII), 15 décembre 2008.

Interruption abusive de services de téléphone et d'Internet par câble

Le demandeur réclame des dommages de 7 000 $ de Vidéotron pour avoir débranché abusivement et sans avertissement son service de téléphonie et d'Internet par câble alors qu'il était client de Vidéotron depuis plus de trois années et pour avoir retardé indûment le rétablissement de ces services après lui

avoir surchargé quelque 421,96 $ en frais d'appels interurbains qu'il ne devait pas. Cette surcharge, selon Vidéotron, s'explique par des appels placés en Angleterre à des numéros de téléphone cellulaire et non filaire. Le tarif est ainsi passé de 0.07 $ à 0.49 $ la minute. Le demandeur n'a jamais été avisé de ce changement.

Vidéotron est un prestataire de services tenu d'agir au mieux des intérêts de son client et ce, avec prudence et diligence. Selon la preuve prépondérante, il ne fait aucun doute dans l'esprit du Tribunal que Vidéotron n'a pas agi de bonne foi et a fait complètement fi des intérêts de son client, un comptable dont le témoignage est apparu sincère et crédible à ses yeux. Lors de ses appels répétés auprès de ses divers services, Vidéotron a toujours laissé faussement croire à son client que les numéros de téléphone qu'il signalait en Angleterre correspondaient à des numéros de téléphone cellulaire. Il est clair qu'il était financièrement préférable pour Vidéotron d'attribuer le tarif de 0,49 $ la minute pour les numéros de téléphone cellulaire en Angleterre que celui de 0,07 $ pour les lignes filiaires et de laisser le soin au client de se débrouiller seul face à une stratégie où le client n'aura jamais raison. Rien ne justifiait la coupure abrupte de service sans préavis alors que le demandeur continuait d'effectuer les paiements réguliers à échéance, coupure survenue par surcroît alors que le demandeur se trouvait en Irak sans possibilité de communiquer avec ses fils laissés seuls à la maison. Le tribunal conclut qu' « avec grand respect pour l'opinion contraire, il s'agit d'un cas d'abus de droit patent de la part de Vidéotron dont la mauvaise foi évidente à l'endroit du demandeur, un homme d'affaires et père de famille, lui a directement causé des dommages pécuniaires et moraux que le Tribunal fixe à 4 000 $ et ce, en fonction des faits mis en preuve et du caractère particulièrement abusif et illégal des agissements de Vidéotron et de ses préposés envers le demandeur, en l'espèce. »

- *Al-Dezeie c. Vidéotron ltée*, 2008 QCCQ 12157 (CanLII), 17 décembre 2008.

Conférence en ligne sur la confiance et les environnements électroniques

Ce séminaire, regroupant des experts canadiens et européens, visait à explorer non seulement les différentes acceptions de la notion de confiance, mais également les mécanismes permettant de la produire dans les environnements électroniques. On peut y voir et entendre des présentations portant sur : *Les politiques de confidentialité, un mécanisme de production de la confiance*, Cynthia Chassigneux; *La confiance, une notion aux multiples définitions*, Jean-Guy Belley, Ejan Mackaay et Daniel Weinstock; *La confiance, une notion aux applications multiples,* Valérie-Laure Bénabou, Nathalie Daigle, Anthony Hémond et Étienne Montéro. Pierre Trudel propose une synthèse des exposés.

- *Confiance et environnements électroniques*, Séminaire d'experts organisé par la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, 20 novembre 2008, en ligne, vidéos et certains textes de présentation.

Générateur de politique de confidentialité

La Chaire L.R. Wilson a mis en ligne un *Générateur de politique de confidentialité* afin d'aider ceux qui ont à mettre en place des politiques de confidentialité dans le cadre de l'exploitation de sites Internet.

Le *Générateur de politique de confidentialité* repose sur un questionnaire permettant au responsable ou au professionnel de consigner des informations pertinentes. En fonction des réponses données, le site génère une politique de protection des renseignements personnels. Cette politique n'est qu'un modèle. Le *Générateur de politique de confidentialité* n'a pas pour fonction de certifier les engagements en matière de protection des renseignements personnels. C'est un outil pour aider dans l'élaboration d'une politique de confidentialité. Le *Générateur de politique de confidentialité* comprend quatre étapes :

- 1ère étape : Informations générales sur l'organisme ou l'entreprise. À cette étape, il

faut préciser le nom et les coordonnées, non seulement de l'organisme ou de l'entreprise, mais également de la personne responsable de la protection des renseignements personnels au sein de l'organisme ou de l'entreprise.

- 2ème étape : Informations générales sur les engagements de l'organisme ou de l'entreprise. À cette étape, il faut préciser – de façon générale – les engagements de l'organisme ou de l'entreprise en ce qui a trait à la protection des renseignements personnels.
- 3ème étape : Informations complémentaires sur les engagements. À cette étape, il s'agit de documenter – de façon spécifique – les engagements de l'organisme ou de l'entreprise en ce qui a trait à la protection des renseignements personnels.
- 4ème étape : Politique de protection des renseignements personnels. En fonction des réponses indiquées aux étapes précédentes, une politique-modèle de protection des renseignements personnels est présentée.

■ Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, *Générateur de politique de confidentialité*.

Le Forum des droits sur l'Internet recommande une ouverture raisonnée pour la publicité pour l'alcool sur Internet – France

La législation française (Loi Évin du 10 janvier 1991) encadrant la publicité pour les boissons alcooliques autorise, par exception et sous certaines conditions, ces publicités dans la presse écrite, à la radio, par affichage et dans les courriers. Avec le développement d'Internet, les acteurs économiques ont investi ce nouveau canal de diffusion pour leurs messages publicitaires. Mais ces pratiques ont été remises en cause par de récentes décisions de justice, laissant ainsi tout un secteur économique dans l'incertitude. Dans ce contexte, les pouvoirs publics réfléchissent à l'actualisation de la loi Évin pour intégrer Internet dans le dispositif légal. Dans ce contexte, le Forum des droits sur l'Internet a publié le 15 décembre 2008 ses recommandations en matière de publicité en ligne en faveur des boissons alcooliques. Ces propositions constituent le premier volet des réflexions du groupe de travail multiacteur du Forum des droits sur l'Internet « Publicité en ligne ».

Les travaux du Forum visent à éclairer la décision publique en faisant des propositions concrètes résultant d'une réflexion approfondie et concertée entre les acteurs parties prenantes (acteurs économiques, société civile et pouvoirs publics). Le principe de « neutralité technologique » a conduit le Forum à considérer que le même régime juridique devait s'appliquer à la radio traditionnelle et en ligne. Dès lors, les conditions de diffusion des messages publicitaires en faveur de l'alcool sur une radio en ligne seraient les mêmes que celles qui s'appliquent aux radios traditionnelles : les émissions diffusées en simultané ou en différé sur Internet ne pourraient pas intégrer des publicités en faveur de l'alcool pendant les tranches horaires non autorisées par la loi. Par contre, le message publicitaire en ligne présente la particularité d'être interactif. Les formats publicitaires sont nombreux et se renouvellent constamment sur Internet. Aussi, préciser dans la loi ou le décret les formats autorisés ne paraît pas pertinent et le Forum recommande de renvoyer à une charte multiacteur l'encadrement des formats de publicité en ligne.

■ Forum des droits sur l'Internet, Recommandation-*Publicité en ligne et alcool*, 15 décembre 2008.

Obligation des sites de conserver les données de connection – France

Le site Legalis.net constate que faute du décret en Conseil d'état prévu à l'article 6-II de la *Loi pour la confiance dans l'économie numérique* (LCEN) définissant les données, la durée et les modalités de conservation, « l'obligation de conservation des données d'identification des créateurs de contenus par les hébergeurs est interprétée de manière très variable selon les juges, même au sein d'une même juridiction. » Par exemple, on relève que dans une décision rendue en référé, la Cour d'appel de Paris est restée très prudente sur la question. Récemment, dans une ordonnance du 7 janvier 2009,

elle a autorisé la société Youtube à communiquer à l'humoriste Raphaël Mezrahi et à la société de production Troyes dans l'Aube les noms d'utilisateurs, leur adresse électronique et l'IP utilisées par les internautes à l'origine de la mise en ligne de vidéos litigieuses dont l'URL avait été identifiée dans des constats. Faute de décret, la cour a conclu que la communication sollicitée ne pouvait être limitée qu'aux documents proposés par Youtube, à savoir ceux qu'elle est susceptible de recueillir au moment de la mise en ligne.

Le même jour, le Tribunal de Grande Instance de Paris (TGI) est arrivé à la même conclusion que la cour d'appel dans une ordonnance de référé relative à une affaire opposant Lafesse à Youtube. Le tribunal a demandé à la plateforme de partage de vidéos de communiquer les données fournies par les éditeurs, à savoir les internautes, notamment les adresses IP et email. Par contre, dans un jugement au fond du 14 novembre 2008, le TGI de Paris a plutôt jugé que Youtube n'avait pas rempli ses obligations d'hébergeur en ne collectant que l'adresse IP, l'adresse email et les pseudonymes des internautes pouvant poster une vidéo. Les juges ont rappelé que la législation impose aux éditeurs, en l'espèce les internautes, de communiquer leurs noms, prénoms, domicile et numéros de téléphone et que c'est aux hébergeurs de leur fournir les moyens techniques nécessaires pour satisfaire cette exigence.

- *Hébergeur : les juges du fond et des référés en désaccord sur l'obligation de collecte de données d'identification des contributeurs*, Legalis.net, 14 janvier 2009.

Responsabilité éditoriale du site qui publie des images à partir d'un flux RSS – France

Dans une ordonnance de référé du 15 décembre 2008, le Tribunal de Grande Instance de Paris condamne un particulier qui avait créé un site Internet important des contenus grâce à des flux RSS. L'usager a été condamné, en tant qu'éditeur, pour atteinte au droit à l'image car il a effectué lui-même le choix du type de contenus à rechercher. Il n'a pas prétendu que des internautes ont pris l'initiative de mettre en ligne des liens litigieux. Les juges en infèrent que la présence sur un site, qui propose des « vidéos porno en folie », d'images de la comédienne concernée, au milieu de contenus similaires, résulte d'un choix éditorial affirmé dès la page d'accueil. Ainsi, la personne qui fournit ce service de communication au public par voie électronique doit en répondre.

Comme le souligne le site Legalis.net, cette ordonnance de référé vient nourrir la jurisprudence émergeante relative à la responsabilité des sites alimentés par des flux RSS. Dans les affaires Lespipoles.com et Dicodunet.com, le TGI de Nanterre avait considéré que ces sites étaient éditeurs en procédant à une analyse de leur implication dans les choix éditoriaux (voir Bulletin d'IT-Can, 20 mars 2008).

- *Claire L. dit K. / Mehdi K.*, Tribunal de grande instance de Paris, Ordonnance de référé, 15 décembre 2008.
- *Responsabilité éditoriale du site qui publie des images à partir d'un flux RSS,* Legalis.net, 19 décembre 2008.

L'exclusivité sur l'Iphone – France

En France, la commercialisation de l'Iphone se fait par l'intermédiaire de l'opérateur de téléphonie mobile Orange en vertu d'un contrat d'exclusivité signé avec Apple. Par une décision récente du Conseil de la Concurrence, cette exclusivité a été suspendue afin de rétablir le libre jeu de la concurrence sur le marché de la téléphonie mobile.

- Sylvain STAUB & Charlotte GIBON, *La fin de l'exclusivité d'Orange sur l'iphone*, Juriscom.net, 9 janvier 2009.

À signaler

- Alain STROWEL et Jean-Paul TRIAILLE, *Google et les nouveaux services – Impact sur l'économie et questions de propriété intellectuelle*, Bruxelles, Larcier, 2008.
- Pierre TRUDEL, « La responsabilité des prestataires intermédiaires d'Internet : l'approche de la législation du Québec », [2008] *Media Lex* 160.

- Pierre TRUDEL, « Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'État en réseau », dans Maria Veronica Pérez ASINARI et Pablo PALAZZI, *Défis du droit de la protection de la vie privée – Perspectives du droit européen et nord-américain*, Bruxelles, Bruylant, 2008, 531-558.