CANADIAN INTERNET LAW UPDATE - 2010*

By Bradley J. Freedman and Robert J.C. Deane
Borden Ladner Gervais LLP
www.blg.com

This paper summarizes selected developments in Internet law that occurred in 2010. In this brief update, it is impossible to present more than an overview of significant developments in several representative areas of Internet law. Reference to current legislation, regulatory policies and guidelines, and case law is essential for anyone addressing these issues in practice.

A. Intellectual Property and the Internet

1. Trade-marks

a. *Mortgagebrokers.com Holdings Inc. v. Mortgage Brokers City Inc.* – Injunction to Restrain Use of Domain Name Refused

Mortgagebrokers.com Holdings Inc. v. Mortgage Brokers City Inc., 2010 ONSC 1797, involved a trade-mark dispute between competing mortgage brokers that were previously affiliated. The plaintiff claimed that the defendants' use of the MORTGAGE BROKERS OTTAWA & Design trade-mark and the mortgagebrokersottawa.com domain name infringed the plaintiff's MORTGAGE BROKERSOTTAWA.COM & Design trade-mark and its mortgagebrokers.com domain name. The plaintiff applied for an interlocutory injunction restraining the defendants from using the mortgagebrokersottawa.com domain name. The defendants maintained that their use of the MORTGAGEBROKERSOTTAWA.COM & Design brand was lawful, and further stated the intention to redesign their website to eliminate any resemblance to the plaintiff's website. The court refused to grant the injunction on various grounds, including the plaintiff's unclean hands (due to an unjustified withholding of commissions owned to defendants), the plaintiff's failure to prove irreparable harm, and the balance of convenience, which favoured allowing the defendants to continue to use the domain name.

b. *Private Career Training Institutions Agency v. Vancouver Career College (Burnaby) Inc.* – Injunction to Restrain Keyword Advertising Refused

Private Career Training Institutions Agency v. Vancouver Career College (Burnaby) Inc., 2010 BCSC 765, involved a dispute over the use of trade-marks and trade names as keywords for Internet advertising. The Agency, the regulatory body for career training institutions in B.C., applied for a permanent injunction restraining Vancouver Career College from using its competitors' business names as keywords for Internet advertising, which the Agency claimed constituted misleading advertising prohibited by the Agency's bylaws. The court dismissed the application, on the basis that the keyword advertising was not false, deceptive or misleading, and in fact was beneficial to Internet users because it provided them with alternative offerings. The court reasoned that the keywords resulted in advertisements that were clearly identified as "sponsored links" that were distinguishable from organic search results. The court accepted the College's argument that keyword advertising is no different than the time-honoured and generally accepted marketing practice of a business locating its advertisement close to a competitor's telephone number in the same directory, so that potential customers of that competitor discover there is another business offering a similar product or service. The court found that the two students who claimed to have been misled by the College's advertisements had been careless.

 This paper is an earlier version of a paper in *Annual Review of Law & Practice*, 2010, Continuing Legal Education Society of British Columbia. The authors acknowledge the assistance of Maria Zeldis, Articled Student, in the preparation of this paper.

2. The Canadian Internet Registration Authority Dispute Resolution Policy

a. Overview

Certain disputes involving alleged bad faith registration of .ca domain names can be resolved by arbitration pursuant to the Domain Name Dispute Resolution Policy (the "**CDRP**") mandated by the Canadian Internet Registration Authority ("**CIRA**"). The CDRP's mandatory administrative dispute resolution process is binding on .ca domain name registrants because it is incorporated by reference into .ca domain name registration agreements. The CDRP is modeled on the Uniform Domain Name Dispute Resolution Policy (the "**UDRP**") mandated by the Internet Corporation for Assigned Names and Numbers and applicable to .com, .org, .net and other domain names. However, the CDRP contains certain provisions that are distinctly Canadian and are designed to improve upon the UDRP in light of its interpretation and practical application.

A complainant must satisfy the CIRA Canadian presence requirements for registrants in respect of the domain name that is the subject of the proceeding or be the owner of the trade mark registered in the Canadian Intellectual Property Office that is the basis of the complaint. A complainant must prove: (i) the disputed domain name is confusingly similar to a mark in which the complainant had rights prior to the date of registration of the domain name and continues to have such rights; (ii) the registrant has no legitimate interest in the domain name; and (iii) the registrant registered the domain name in bad faith. The CDRP provides detailed and exhaustive definitions of each required element.

b. CDRP Decisions

There were 19 CDRP decisions, involving 21 domain names, issued during 2010. A complete list is available at www.cira.ca. Complaints continue to be upheld more frequently than they are dismissed. During 2010, 14 orders were made requiring that domain names be transferred to complainants, while 7 orders were made dismissing complaints.

The 2010 CDRP decisions highlight five noteworthy issues:

- The CDRP is limited in scope, and will not apply to all disputes relating to domain names: *Warren Miller Entertainment Inc. v. Willi Vogl & Associates Ltd.*, CIRA No. 159; *Toyota Canada Inc. v. Sproul*, CIRA No. 152; *Vancouver Community College v. Eminata Group*, CIRA No. 148.

- A complaint will fail if it is not supported by sufficient evidence for each required element of the CDRP: *AM Ford Sales Ltd. v. Canada One Auto Group*, CIRA No. 158; *AOL Canada Inc. v. Anderson*, CIRA No. 157.

- The fact that a domain name registrant expressly or implicitly invited a complainant to make an offer to purchase or rent a domain name is evidence that the domain name was registered primarily for the purpose of selling it to the complainant: *DKH Retail Limited v. Facciolo*, CIRA No. 155; *Carlton University Students Association Inc. v. Essiambre*, CIRA No. 153; *Microsoft Corporation v. Guo*, CIRA No. 143; *Zuffa LLC v. Cox*, CIRA No. 161.

- The addition of generic terms will not distinguish a domain name from a trade-mark: *LEGO Juris A/S v. Carswell*, CIRA No. 150; *Microsoft Corporation v. Guo*, CIRA No. 143.

- There continues to be inconsistency regarding the appropriate test for confusing similarity between the complainant's trade-mark and the disputed domain name. Some panels appear to apply a standard contextual confusion test (*AM Ford Sales Ltd. v. Canada One Auto Group*, CIRA No. 158; *LEGO Juris A/S v. Carswell*, CIRA No. 150; and *The Hospital for Sick Children v. Toronto Sick Children Society*, CIRA No. 145) while other panels apply a test of mistake based

upon first impression and imperfect recollection (*DKH Retail Limited v. Facciolo*, CIRA No. 155; *Microsoft Corporation v. Guo*, CIRA No. 143; and *Fitness Anywhere Inc. v. Bannerfrench*, CIRA No. 160).

3. Copyright

a. *Shaw Cablesystems G.P. v. Society of Composers, Authors and Music Publishers of Canada* – Online Streaming is "Communication of the Work to the Public"

Shaw Cablesystems G.P. v. Society of Composers, Authors and Music Publishers of Canada, 2010 FCA 220, involved an application by several Internet service providers ("**ISPs**") for judicial review of a Canadian Copyright Board decision (known as the SOCAN Tariff 22A decision) regarding the application of a copyright tariff to Internet music downloads. The ISPs appealed the Board's decision that the transmission of a musical work by an online music service was a "communication of the work to the public by telecommunication" within the meaning of *Copyright Act* s. 3(1)(f). The ISPs argued that a communication "to the public" required a simultaneous transmission of the same music file to different members of the public, and therefore a music download by an individual was a private communication that was not subject to the tariff. The court upheld the Board's decision, reasoning that simultaneity is not required, and that whether or not a communication is "to the public" was a function of only two factors: the intention of the communicator to communicate to the public, and the reception of the communication by at least one member of the public. The court held that the communicator's intention could be inferred from the circumstances, including the volume of transmissions and the context in which they were made, but noted that volume of transactions, in and of itself, did not transform private communications into communications to the public. The court also held that if there is an intention to communicate a work to the public, then every communication of the work, starting with the first, is a communication to the public.

b. *Society of Composers, Authors and Music Publishers of Canada v. Bell Canada* – Application of "Fair Dealing" Exception to Online Music Previews

Society of Composers, Authors and Music Publishers of Canada v. Bell Canada, 2010 FCA 123, involved an application by SOCAN for judicial review of a Canadian Copyright Board decision regarding the application of a copyright tariff to Internet music downloads. SOCAN appealed the Board's decision applying a "fair dealing" exception to the SOCAN tariff to permit users to sample a free preview of a song excerpt before purchasing the song over the Internet. The court upheld the Board's decision, reasoning that a free preview of a 30-second long excerpt of a song constituted fair dealing for the purpose of "research" within the meaning of section 29 of the *Copyright Act*, and therefore did not require the payment of royalties. The court agreed with the Board's decision that the concept of "research" must be given a large and liberal interpretation in order to ensure that users' rights are not unduly constrained, and that the purpose of the preview was to be considered from the point of view of the person for whom it is intended - the consumer. The court also agreed with the Board's decision that, in assessing the fairness of the previews, the "amount of dealing" was the length of each preview in proportion to the length of the complete work. On December 23, 2010, the Supreme Court of Canada granted SOCAN's application for leave to appeal.

c. *Society of Composers, Authors and Music Publishers of Canada v. Bell* Canada – Application of Copyright Tariff to Internet Simulcasts

Society of Composers, Authors and Music Publishers of Canada v. Bell Canada, 2010 FCA 139, involved an application by SOCAN for judicial review of a Canadian Copyright Board decision regarding the application of a copyright tariff to Internet simulcasts of various radio and television services. The Board held that the current tariff included Internet simulcasts, and refused to specify a royalty rate applicable to

a residual category of "Other Sites". The court held that the Board's decisions were not unreasonable, particularly in light of the limited evidence presented by SOCAN.

d. *Entertainment Software Assn. v. Society of Composers, Authors and Music Publishers of Canada* – Application of Copyright Tariff to Music Included in Game Downloads

Entertainment Software Assn. v. Society of Composers, Authors and Music Publishers of Canada, 2010 FCA 221, involved an application by ESA for judicial review of a Canadian Copyright Board decision regarding the application of a copyright tariff to Internet music downloads. ESA appealed the Board's decision that the music download tariff applies to the downloading of a video game that includes music, which is usually a small portion of the overall software program. The court upheld the Board's decision that there is no *de minimis* rule in relation to the certification of copyright tariffs, and that SOCAN was entitled to a tariff in respect of music included in video game downloads. The ESA has applied to the Supreme Court of Canada for leave to appeal.

4. Patents

a. *Amazon.com Inc. v. Canada (Attorney General)* – "One-Click" E-Commerce Website is Patentable Business Method

Amazon.com Inc. v. Canada (Attorney General), 2010 FC 1011, involved an appeal of a decision of the Canadian Commissioner of Patents denying Amazon.com's application to patent its business method (one-click Internet shopping) on the basis that it was not patentable subject matter. The court allowed the appeal, holding that a business method can be patentable subject matter in appropriate circumstances. The court held that the Commissioner erred in adopting a policy role and excluding business methods patents. The court ruled that there is no exclusion for "business methods" that are otherwise patentable, nor is there a "technological" test under Canadian jurisprudence. The court sent the matter back for expedited re-examination with a direction that the claims constituted patentable subject matter.

B. Privacy

1. *R. v. McNeice* – Warrant Assumed to Have Been Made by Reference to *PIPEDA*

In *R. v. McNeice*, 2010 BCSC 1544, McNeice applied to quash a search warrant authorizing the search of his home and computer. McNeice was charged with accessing and possessing child pornography. A police investigation in Germany led Canadian police to an Internet service provider in Canada, which then provided police with McNeice's address and name. Canadian police then obtained the search warrant. The accused argued that the information used to obtain the search warrant omitted any reference to the *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***"), which would have alerted the issuing Justice of the Peace to question whether the statute had been complied with. The court rejected that argument, on the basis that the Justice of the Peace was legally trained and experienced, and would know of the modest formal requirements of *PIPEDA* in this context. The court dismissed the application.

C. Regulatory Matters

1. Bill C-28 – the *Fighting Internet and Wireless Spam* bill

On December 15, 2010, the Government of Canada enacted Bill C-28 – the *Fighting Internet and Wireless Spam* bill, with the stated purpose of promoting the efficiency and adaptability of the Canadian economy by regulating certain activities (including spam, phishing and spyware) that discourage the use of electronic commerce. The *Act* is a revised version of the proposed *Electronic Commerce Protection Act*, which was originally introduced to Parliament in April 2009 and addresses recommendations of the

Canadian government's Task Force on Spam. The Act will come into force on a date determined by the government, and likely after required regulations have been enacted.

Following is a summary of some of the highlights of the Act:

- The Act contains anti-spam provisions that prohibit commercial electronic messages (including email and instant messaging) unless: (a) the recipient has consented to receive the message; and (b) the message complies with specified formalities, including disclosure of information regarding the actual and beneficial sender of the message and an effective and timely unsubscribe mechanism. The prohibition applies to electronic messages that seek consent to receive other electronic messages. The prohibition applies to the person who actually sends the message and all persons on whose behalf the message is sent. The prohibition does not apply to noncommercial messages. There are also various exceptions for commercial messages, including commercial electronic messages that are interactive two-way voice communications between individuals, facsimile messages, and voice recordings to a telephone account. There is a three-year transition provision for implied consent in limited circumstances.

- The Act contains anti-phishing provisions that prohibit a person, in the course of commercial activity, from altering the transmission data in an electronic message so that the message is delivered to a destination other than or in addition to the destination specified by the sender, without the sender's express consent. The consent must be informed (based upon prescribed information disclosure), and an effective and timely consent withdrawal mechanism must be provided.

- The Act contains anti-spyware/malware provisions that prohibit a person, in the course of commercial activity, from installing any computer program on any other person's computer system, or causing that computer program to send an electronic message from the computer system, without the consent of the owner or authorized user of the computer system. In most circumstances, the required consent must be express and informed (based upon prescribed information disclosures, including the function and purpose of the computer program), and an effective and timely consent withdrawal mechanism must be provided. There are limited exceptions that permit implied consent to the installation of legitimate computer software. There is a three-year transition provision for implied consent in limited circumstances.

- The Act amends *PIPEDA* to prohibit the unauthorized collection of an individual's electronic address or personal information by use of a computer program designed for collecting that information or by unauthorized access to a computer system, or the use of an electronic address or personal information collected in that manner, without the individual's consent.

- The Act amends the Canadian *Competition Act* to add new provisions prohibiting the sending of an electronic message that contains false or misleading information regarding the sender or subject matter of the message, false or misleading information in the content of the message, or false or misleading information regarding a source of data on a computer system (including a URL). The message recipient need not have been deceived or misled by the message for the provisions to apply, and they are not limited to commercial electronic messages.

- The Act gives the CRTC broad powers to investigate and impose substantial administrative monetary penalties for violations of the Act – up to $1 million for an individual and up to $10 million for an organization – in order to promote compliance with the Act. The factors to be considered in assessing penalties include the nature and scope of the violation, past violations, the financial benefits of the violation, and ability to pay. Regulations may have the effect of substantially increasing maximum fines by providing that a contravention of the Act constitutes a

separate violation for each day that it continues. False and misleading electronic messages are subject to administrative enforcement by the Competition Bureau or criminal prosecution, with severe penalties – an unlimited fine and up to 14 years in jail for conviction on indictment, or a fine not exceeding $200,000 and up to one year in jail for summary conviction.

- A violation of the Act is not a criminal offence, and is not punishable by imprisonment. Corporate officers and directors can be held personally liable for corporate violations, and employers can be held liable for violations committed by their employees or agents acting within the scope of their employment or authority. Due diligence to prevent the commission of the violation is a defence.

- The Act gives a private right of civil action to businesses and consumers affected by a violation of the Act, the unlawful collection, use, or disclosure of personal information in violation of *PIPEDA*, or misleading electronic messages in violation of the *Competition Act*. The civil action may be brought against the persons who committed the violation and all other persons vicariously liable for the violation. A private right of action is not available if the violation is already subject to an undertaking or a notice of violation issued by the CRTC. The remedies available in a private action include compensation for loss, damage, and expense plus an additional payment of up to $200 for each contravention to a maximum of $1 million for each day a contravention occurred. The private action remedy is modeled on similar legislation in the United States, where courts have issued multi-million dollar judgments against spammers.

2. *Re. Broadcasting Act* – ISPs Generally not "Broadcasting Undertakings" Subject to CRTC Jurisdiction

Re. Broadcasting Act (Canada), 2010 FCA 178, involved an application by the Canadian Radio-television and Telecommunications Commission to determine whether ISPs carry on "broadcasting undertakings" subject to the *Broadcasting Act* when they provide their customers with Internet access to third party broadcasting services. The court held that retail ISPs do not carry on "broadcasting undertakings" when they provide access through the Internet to third party broadcasting content that they do not control. The court noted that its conclusion was based on the content-neutral role of ISPs, and would have to be reassessed if that role were to change.

D. Internet Defamation

1. *Aldelo Systems Inc. v. Sinclair* – Broad Injunction to Restrain Internet Defamation Refused

Aldelo Systems Inc. v. Sinclair, 2010 ONSC 5229, involved a dispute between the plaintiff and a disgruntled customer over critical and disparaging website postings (including on the website aldeloripoff.com) that the plaintiff claimed were defamatory. The plaintiff applied for an interlocutory injunction restraining the defendant from making any statement, or publishing any information, regarding the plaintiff. The court refused to grant the injunction on the basis that the plaintiff had not shown that it would suffer irreparable harm if the injunction was not granted. The court also held that the balance of convenience weighed against the injunction, particularly given the defendant's right to freedom of expression and the public interest in the free exchange of ideas and information.

2. *Vigna v. Levant* – Application of "Responsible Communication" to Blog Postings

In *Vigna v. Levant*, 2010 ONSC 6308, the defendant posted a comment in his blog alleging that the plaintiff lied when requesting that a hearing before the Canadian Human Rights Commission be adjourned. The defendant was a long-time critic of human rights commissions, and claimed that he was exercising his right of free expression as guaranteed by s. 2(b) of the *Charter*. The court considered whether the new defence of responsible communication on matters of public interest applied to blog postings and other online media. Applying the Supreme Court of Canada's decision in *Grant v. Torstar*,

2009 SCC 61, the court held that the laws of defamation, including the defence of responsible communication on matters of public interest, applied to the articles written by the defendant and posted on his Internet blog. However, the defence could not be established on the facts. The court held that the statements were defamatory and not protected by any defence, and ordered the defendant to remove all defamatory blogs and pay damages in the amount of $25,000.

3. *Black v. Breeden* – Real and Substantial Connection Between Internet Postings and Ontario

In *Black v. Breeden*, 2010 ONCA 547, the defendants sought to overturn an order confirming that the Ontario Superior Court of Justice properly exercised jurisdiction to determine Black's claims of defamation. Black filed six libel actions in Ontario in respect of statements posted on the Hollinger International website. The defendants in the actions were directors, advisors and a vice president of Hollinger, a publicly traded company headquartered in Chicago. Black, who was Hollinger's chairman, alleged that press releases and reports issued by the defendants contained defamatory statements that were downloaded, read and republished in Ontario by three newspapers, and damaged his reputation in Ontario. The defendants brought a motion to stay the actions on the ground that the Ontario court did not have jurisdiction, or alternatively that Ontario was not the convenient forum. The defendants argued that there was no real and substantial connection between Ontario and the actions, and that the more appropriate forum was either New York or Illinois. The motions judge held that the Ontario court had jurisdiction over the actions and Ontario was the convenient and appropriate forum. While the statements in question may have been made in the United States, they were republished in Ontario and were alleged to have caused injury in Ontario. The connection between Black and Ontario was significant and he had long-standing ties to Ontario. The American defendants could be connected to Ontario, because it was reasonably foreseeable to the defendants that the allegedly defamatory press releases would be downloaded and published in Ontario and would result in damage to Black's reputation in Ontario.

The Court of Appeal held that the motions judge did not err in finding that the alleged tort was committed in Ontario. There was evidence that the defendants targeted and directed their statements to the jurisdiction of Ontario. The press releases posted on the Internet specifically anticipated that the statements would be read by a Canadian audience and provided contact information for Canadian media. The facts relevant to Black's claim relating to publication in Ontario and the damage to Black's Ontario reputation formed a significant connection between Black's claims and Ontario. Further, as Black's claims related to statements published in Ontario and his actions were limited to damages to his reputation in Ontario, the motions judge correctly concluded that it would be unfair to deprive him of a trial before the community in which his reputation had been damaged. In addition, there was no unfairness in holding the defendants accountable for the accuracy of statements that were widely disseminated over the Internet and specifically directed to Canadian media. The Supreme Court of Canada granted leave to appeal on December 16, 2010.

4. *National Bank of Canada v. Weir* – Injunction Granted Due to Concerns About Diffusion of Defamatory Statements Online

In *National Bank of Canada v. Weir*, 2010 QCCS 402, the Bank sought an interlocutory injunction broadly restraining Weir from publishing any defamatory comments regarding the Bank, its affiliates, subsidiaries, directors, officers, management, employees, representatives or shareholders. Weir disseminated the allegedly defamatory statements by way of Internet blog postings on a website that claimed to have one million unique users every month and 77 million page views every month. The court noted that injunctive relief on an interlocutory basis to restrain abusive and defamatory comments is rarely granted. However, the facts and circumstances in the present case constituted an exception. The court took particular note of the problems presented by widespread use of the Internet as a means of spreading defamatory statements. The court allowed the Bank's application for interim relief and ordered Weir to refrain from publishing any defamatory statements about the Bank by any media whatsoever.

5. *Canadian National Railway Co. v. Google Inc*. – Host Ordered to Block Access to Defamatory Blog

In *Canadian National Railway Co. v. Google Inc*., 2010 ONSC 3121, the plaintiff applied for an interim injunction requiring Google to dismantle the defendants' blog, which Google hosted through its Blogspot subsidiary. Google had temporarily blocked the site but was not prepared to continue to do so without an order, which it did not oppose. Following *Barrick Gold Corp. v. Lopehandia* (2004), 71 O.R. (3d) 416, in which the Ontario Court of Appeal held that the novel nature and broad impact of the publication of defamatory material on the Internet affects the test for granting an injunction, the court considered that the mode and extent of publication was a particularly significant consideration in determining whether to grant the injunction. The court found that the blog referred to the plaintiff as a hustler, compared it to Enron and suggested it had defrauded and bribed the government. The blog also accused specific executives and senior employees of impropriety. The court held that the words used were clearly capable of damaging the plaintiff's reputation, the defendants had not shown any intention of justifying their blog and Google did not object to the motion. Google and the defendants were therefore ordered to remove the blog and any other defamatory content.

6. *Hunter Dickinson Inc. v. Butler* – Permanent Injunction Issued Against Internet Defamation

In *Hunter Dickinson Inc. v. Butler*, 2010 BCSC 939, the plaintiff applied for summary judgment and a permanent injunction restraining Butler from publishing defamatory materials. Butler admitted to authoring numerous blog postings alleging illegal activities on the part of the plaintiff. The court allowed the application for summary judgment, and granted the injunction, because Butler admitted he made the postings and they were intended to be viewed by the public, the statements were clearly defamatory, and that Butler chose to publish his statements on a website he knew was frequently accessed by investors and potential investors in order to inflict the most damage possible. Relying upon *Barrick Gold Corp. v. Lopehandia* (2004), 71 O.R. (3d) 416 (C.A.), the court restrained Butler from "disseminating, posting on the Internet or publishing further defamatory statements".

7. *Sauvé v. Canada* – Linked Website Not Liable for Defamatory Statements on Originating Website

In *Sauvé v. Canada*, 2010 FC 734, the plaintiff alleged that the RCMP was liable for defamatory statements posted about him on a website – Zoominfo – which was linked to a website maintained by someone associated with the RCMP (and which used the RCMP's name and marks). The court held that the comments were not defamatory. Moreover, the plaintiff had failed to establish any connection between the posting on Zoominfo and the RCMP-associated website, apart from the link, which was not within the latter's control. The action was dismissed.

E. Human Rights

1. *Jodhan v. Canada (Attorney General)* – Website Technology Infringed Charter Rights

Jodhan v. Canada (Attorney General), 2010 FC 1197, involved a plaintiff who was visually impaired, and who was unable to access information and a number of services on federal government websites, including the Job Bank and the online 2006 Census. She applied for a declaration that standards implemented by the federal government for providing visually impaired Canadians with access to government information and services on the Internet violated her rights under s. 15(1) of the *Charter*. The court held that the plaintiff's inability to access online governmental department websites represented a system-wide failure by government to make websites accessible. The government's failure to monitor and ensure compliance with its own 2001 accessibility standards infringed the 15(1) *Charter* rights of the plaintiff and other visually impaired persons, because it discriminated against them on the basis of their

physical disability. The court held that the government had a constitutional obligation to bring its websites into compliance with the *Charter* within 15 months.

F. Practice Issues

1. *A.B. v. Bragg Communications Inc.* – ISP Ordered to Disclose Identity of Person Engaged in Facebook Defamation

A.B. v. Bragg Communications Inc., 2010 NSSC 215, involved an application requiring the defendant Internet service provider to disclose the identity of a user who the plaintiff alleged was responsible for creating a fake Facebook profile that defamed the plaintiff. The defendant did not oppose the application. The court ordered the requested disclosure, on the basis that there was a *prima facie* case of defamation, there was no other means by which the plaintiff could obtain the required information, the author of the defamatory Facebook profile did not have a reasonable expectation of anonymity in the circumstances, and the public interest favoured disclosure.

2. *Frangione v. Vandongen* - Party Ordered to Disclose Contents of Private Portion of Facebook Page, But Not Other Electronically Stored Information

Frangione v. Vandongen, 2010 ONSC 2823, involved a lawsuit for damages suffered by the plaintiff as a result of two motor vehicle accidents. The defendant applied for an order requiring the plaintiff to disclose all data on his personal computer and all information from the private areas of his Facebook page. The plaintiff resisted production on the basis that his personal computer was used by other family members and his Facebook page contained privileged and private information. The court ordered the plaintiff to preserve and produce all information from the private parts of his Facebook page, because it was relevant to the matters in dispute (including the plaintiff's physical injuries) and was not subject to legal privilege or overriding privacy rights. The court refused to order the plaintiff to produce his entire computer hard drive for a forensic examination, because it contained private information of other users and there was no evidence that it contained relevant documents that had not been produced. The court also refused to order the plaintiff to produce all metadata from his computer hard drive to reveal the amount of time the plaintiff used his computer each day, because that information would have minimal probative value and therefore the privacy interest of the plaintiff and his family outweighed the interests of the defendant.

3. *Warman v. National Post Co.* – Independent Expert Permitted to Review Hard Drive

Warman v. National Post Co., 2010 ONSC 3670, involved a dispute over alleged defamatory website postings. One of the defendants claimed that the postings were true, and asserted that the proof would be found on the plaintiff's computer hard drive. The defendant sought production of a mirror image of the plaintiff's computer hard drive. Applying the rule of proportionality, the court refused to order production of the plaintiff's entire hard drive, on the basis that it contained irrelevant information, the information could be used for a collateral purpose, and the action was a simplified proceeding. Nevertheless, the court ordered that the hard drive be reviewed by an independent expert to identify relevant metadata, including deleted documents.

4. *Facebook v. Guerbuez* – Foreign Spam Judgment Enforced in Quebec

Facebook v. Guerbuez, 2010 QCCS 4649, involved the enforcement in Quebec of a California judgment for $800 million in damages issued in a lawsuit relating to the defendant's unlawful collection of Facebook users' personal information and the use of that information to send spam. The main issue in the Quebec case was whether or not the California order was "contrary to public order as understood in international relations," which, under the *Quebec Civil Code*, would make it unenforceable. The Quebec

court enforced the California judgment on the basis that it was not inconsistent with penalties that might be imposed under Canadian law.

5. *Yazdani v. Canada (Minister of Citizenship and Immigration) et al* – Risk of Error in Sending Important Notices by Email Only

Four immigration cases in 2010 canvassed the issue of which party bears the risk of non-delivery when email is used to send important notices: *Yazdani v. Canada (Minister of Citizenship and Immigration),* 2010 FC 885; *Abboud v. Canada (Minister of Citizenship and Immigration),* 2010 FC 876, *Alavi v. Canada (Minister of Citizenship and Immigration),* 2010 FC 969; and *Zare v. Canada (Minister of Citizenship and Immigration),* 2010 FC 1024. Each case was a judicial review of an immigration officer's refusal of applications for permanent residence visas. The reviewing officer sent emails to the applicants seeking further information regarding their applications and, when the information was not provided, the applications were rejected. The court allowed the applications and remitted the matters to different reviewing officers for re-determination, holding that the applicants, through no fault of their own or of their consultant, were not aware of the requests, the emails were not deleted or blocked by a spam filter, and there was no evidence that the applicants were at fault for the failed email communication. The email communication system failed for an undetermined cause or causes. Holding that the officer chose to send an important and crucial notice to the applicants by email without safeguards in place, the court considered that it was appropriate for the Minister to bear the consequences of the email transmission failure. It is important to note that similar issues regarding the delivery of records and information by email are addressed in British Columbia by s. 18 of the *Electronic Transactions Act*.

G. Cybercrime and Regulatory Offences

1. New Identity Theft Laws

In October 2009, Royal Assent was given to Bill S-4, which amends the *Criminal Code* (Canada) to add a number of offences relating to identity theft. The amendments include a new definition of "identity information" (which includes biometric information, electronic signatures, user names, and passwords), and establish three new offences: (a) identity theft (obtaining and possessing identity information intended to be used to commit an indictable offence that includes fraud, deceit or falsehood); (b) trafficking in identity information (the transfer or sale of another person's identity with knowledge of or recklessness as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood); and (c) unlawfully possessing or trafficking in government-issued identity documents that contain information of another person. The new offences carry a five year maximum term of imprisonment. In addition, other amendments clarify and expand existing *Criminal Code* offences regarding credit card offences, mail theft, trafficking in forged documents, and identity fraud. The amendments also allow courts to order offenders to repay victims the costs of re-establishing their identity. The amendments came into force on January 8, 2010.

2. *R. v. R.J.S.* – Accused Acquitted of Unlawful Use of Internet Services

In *R. v. R.J.S.*, 2010 NSSC 253, the accused was charged with sexual offences and with the illegal use of an Internet service, contrary to s. 342.1(1)(a) of the *Criminal Code*. The accused was arrested as the result of a sting operation in which an officer posed as a 13-year-old boy. The accused found the officer in a teen chat room and they began chatting privately on MSN. The IP address used by the accused for the conversations was registered to another individual and the accused accessed it through that individual's unsecured wireless network. The accused testified that he believed the wireless service belonged to his landlord and that access was included in his rent. The landlord testified that the building had a wired Internet service which tenants were required to apply for and activate if they wanted Internet service. The

court convicted the accused of the sexual offences but acquitted him of unlawful Internet usage on the basis that the accused's explanation about his Internet access raised a reasonable doubt.

3. *R. v. Juneja* – Website Advertisements Linked to Accused

R. v. Juneja, 2010 ABCA 262, was an appeal by the accused from convictions on three counts of living on the avails of prostitution. The evidence included advertisements for certain establishments, including advertisements posted on explicit websites. The accused raised several grounds of appeal, including that the advertisements were not shown to have been inserted, created or commissioned by the accused. The court dismissed the appeal. Although the court recognized that it was theoretically possible that someone could have posted the advertisements for the benefit of the accused's establishments, the court held that the issue was only one of admissibility. On that basis, the court held that the evidence concerning the websites was admissible and, taken together with other admissible evidence, proved an overwhelming case against the accused.
