CANADIAN INTERNET LAW UPDATE – 2012*

By Bradley J. Freedman
Borden Ladner Gervais LLP
www.blg.com

This paper summarizes selected developments in Internet law during in 2012. This paper is an overview of significant developments rather than an exhaustive review. Reference to current legislation, regulatory policies and guidelines, and case law is essential for anyone addressing these issues in practice.

A. Trademarks and the Internet

1. Liability for Infringing Domain Name

Dentec Safety Specialists Inc. v. Degil Safety Products (1989) Inc., 2012 ONSC 4721, involved a domain name dispute between direct business competitors (owned and controlled by estranged brothers). The plaintiff used the domain name dentecsafety.com for its website. The defendant registered the domain name dentecsafety.ca, and for a five-month period caused the domain name to automatically redirect users to the defendant's website at degilsafety.com. The court held that the defendant's conduct constituted a passing-off because the disputed domain name was a misrepresentation to the public that there was a business connection or association between the parties that caused or was likely to cause confusion among ordinary average customers as to whether the goods sold by the defendant were those of the plaintiff and which resulted in damage (as a result of lost sales and customers) to the plaintiff. The court awarded the plaintiff $10,000 in compensatory damages, even though there was no clear and direct evidence as to the sales, customers, or business lost by the plaintiff or of any confusion on the part of any member of the public as a result of the defendant's passing-off. The court refused to make an award of punitive damages.

2. Settlement of Metatag Dispute

Skipper Online Services (SOS) Inc. v. 2030564 Ontario Inc., 2012 ONSC 1852, affirmed 2012 ONCA 606, involved a dispute over confusing website metatags (hidden keywords describing website content). The parties settled the dispute by way of a settlement agreement that prohibited each party from using as website metatags certain specified English and French phrases (including "examen de bateau") or words or any "reversals, misspellings, translations or plurals thereof". The defendant's list of prohibited metatags included "examen de bateau". After the settlement, the defendant used the metatags "boat exam" and "boating exam", and the plaintiff sued to enforce the settlement agreement, claiming that "boat exam" and "boating exam" were each translations of the specifically prohibited metatag "examen de bateau". The defendant argued that "boat exam" and "boating exam" were not in the list of specifically prohibited metatags and the reference to "translations" was intended to be limited to translations to a language other than English or French, because the specifically listed prohibited metatags were in English and French. The court rejected the defendant's argument, reasoning that the word "translation" included any translation in any language.

3. Canadian Court retains Jurisdiction over Domain Name Dispute

Tucows.com Co. v. Holley Performance Products, Inc., 2012 ONSC 1319, involved a dispute over the plaintiff's registration of the domain name earls.com, which the defendant claimed infringed the defendant's trademarks. The defendant commenced an arbitration under the *Uniform Domain-Name Dispute-Resolution Policy* ("UDRP"), and the plaintiff responded by commencing a lawsuit in the Ontario Superior Court of Justice seeking a declaration that the plaintiff was lawfully entitled to use the domain name in Ontario. The UDRP proceeding was then dismissed on the basis that the dispute was subject to the Ontario lawsuit. The defendant then commenced a lawsuit in Kentucky seeking remedies for cybersquatting, trademark infringement and unfair competition. The Kentucky court dismissed the plaintiff's application to have the Kentucky lawsuit stayed in favour of the Ontario lawsuit, reasoning that both lawsuits could proceed in parallel. The defendant then applied to the Ontario court for an order staying the Ontario lawsuit pending the outcome of the Kentucky lawsuit. The Ontario court dismissed the defendant's application on the basis that the court had jurisdiction over the lawsuit based upon a real and substantial connection with Ontario

(the plaintiff is in Ontario, its activities are carried on in Ontario, and the defendant has activities in Ontario) and the balance of convenience did not favour Kentucky courts.

4. Advice Website and Domain Name Non-infringing

Insurance Corp. of British Columbia v. Stainton Ventures Ltd., 2012 BCSC 608, involved a dispute over the defendant's *ICBCadvice* website—a marketing tool for a commercial guide to dealing with ICBC and for legal services—and the related domain names icbcadvice.com and icbcadvice.ca. ICBC claimed that the website and domain names violated ICBC's official mark ICBC (contrary to *Trade-marks Act* ss. 9 and 11), and constituted passing-off (contrary to *Trade-marks Act* s. 7(b) and common law) and misleading advertising (contrary to *Competition Act* s. 52). ICBC did not make any claims regarding the substantive content of the defendant's website. The court held that the domain names did not so nearly resemble the official mark ICBC as to be likely to be mistaken for it. The court reasoned that a British Columbian would likely understand the domain names as identifying the subject matter, rather than the owner, of the website. The court held that the defendant's use of the ICBC acronym throughout the website was a nominative use (to identify ICBC) rather than a trade-mark use (to identify and distinguish the defendant's products) and therefore did not infringe the official mark ICBC. The court held that the defendant's domain names and website did not constitute passing-off, because the average consumer would not be deceived into thinking that the website was associated with or approved by ICBC. The court reasoned that the tendency of search engines to display the defendant's website in response to an Internet search for "ICBC" reflected the underlying search algorithm and search-engine marketing and was not evidence of consumer confusion. The court also held that the defendant's domain names and website did not constitute a false or misleading representation contrary to the *Competition Act*, because they were not likely to deceive the public.

5. Trademark Use through Website Display

HomeAway.com, Inc. v. Hrdlicka, 2012 FC 1467, involved an application to expunge a trade-mark registration on the basis that the applicant had prior rights in the trade-mark based upon the applicant's use of the trade-mark in association with its vacation rental services business. The applicant had used the trade-mark on its U.S.-based website, which was accessed by Canadian customers. The court held that the applicant had used the trade-mark in connection with the applicant's services before the respondent applied to register the trade-mark because the trade-mark was displayed on the computer screen when the applicant's website was accessed by Canadians. The court reasoned that a trade-mark that "appears on a computer screen website in Canada, regardless where the information may have originated from or be stored, constitutes for *Trade-marks Act* purposes, use and advertising in Canada". The court also held that the respondent did not have a good faith intention to use the trade-mark in a legitimate commercial way in Canada; rather, the respondent's intention was to extort money or other consideration from the applicant. The court ordered the trade-mark registration expunged and awarded costs to the applicant.

6. Brand Protection and Social Media

Industries Lassonde inc. v. L'Oasis D'Olivia inc., 2010 QCCS 3901 and 2012 QCCA 593, involved a hard-fought trade-mark dispute over two brands that both include the word "oasis". The trial court dismissed the plaintiff's claims against the defendant and awarded the defendant substantial costs and punitive damages under Quebec's *An Act to amend the Code of Civil Procedure to prevent improper use of the courts and promote freedom of expression and citizen participation in public debate*. The Court of Appeal reversed the trial judge's findings and set aside the award of costs and punitive damages. The appellate decision was reported by the press, which characterized the plaintiff as a corporate bully. The plaintiff then faced an onslaught of public condemnation through social media, including extensive critical postings on Twitter and the plaintiff's official Facebook page. According to media reports, in response to the adverse public reaction on social media, the plaintiff's senior representatives met with the defendant's owner and negotiated a settlement.

7. Jurisdiction over Domain Name Dispute

In *Tucows.com Co. v. Lojas Renner S.A.*, [2011] S.C.C.A. No. 450 (QL), the Supreme Court of Canada dismissed an application for leave to appeal a decision of the Ontario Court of Appeal (2011 ONCA 548) in which the court held that an Ontario court had jurisdiction over a dispute regarding ownership of a domain name. The Court of Appeal had based its decision on a determination that the dispute had a real and substantial connection with Ontario (because the domain name was personal property in Ontario), and therefore service of the statement of claim on the defendant outside Ontario was valid.

8. Canadian Domain Name Arbitrations

(a) Overview

Certain disputes involving alleged bad faith registration of .ca domain names may be resolved by arbitration pursuant to the Domain Name Dispute Resolution Policy (known as 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 (known as the "UDRP") that applies 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.

To invoke the CDRP, a complainant must satisfy the CIRA Canadian presence requirements for registrants with respect to the disputed domain name, or be the owner of the trade-mark registered in the Canadian Intellectual Property Office that is the basis of the complaint. To succeed in a CDRP proceeding, a complainant must prove that: (a) the disputed domain name is confusingly similar to a mark in which the complainant had rights prior to the date of registration of the disputed domain name and continues to have such rights; and (b) the registrant registered the disputed domain name in bad faith; and must provide "some evidence" that (c) the registrant has no legitimate interest in the disputed domain name. Even if a complainant proves (a) and (b) and provides some evidence of (c), the registrant will succeed in the proceeding if the registrant proves that the registrant has a legitimate interest in the disputed domain name. The CDRP provides non-exhaustive lists of circumstances that demonstrate bad faith registration of a disputed domain name and legitimate interest in a disputed domain name.

(b) Decisions

There were 38 CDRP decisions, involving 44 domain names, issued in 2012. A complete list is available at www.cira.ca. Complaints continue to be upheld more frequently than they are dismissed. During 2012, 28 complaints were successful and 10 complaints were dismissed.

The 2012 CDRP decisions illustrate the following:

- The criteria for finding bad faith registration added to CDRP paragraph 3.5(d) in 2011—intentionally attempting to attract Internet users for commercial gain by creating a likelihood of confusion—is a common basis for a successful complaint (*TWENGA, S.A. v. Privacy Protected*, CIRA No. 177; *Ontario Power Authority v. The Urban Environment (Toronto)*, CIRA No. 179; *Cointreau v. Netnic Corporation*, CIRA No. 180; *General Motors LLC v. Wilson*, CIRA No. 182; *Etro S.p.A. v. Segarra*, CIRA No. 183; *HMV (IP) Limited v. Mateescu*, CIRA No. 185; *Oakley Inc. v. yayang*, CIRA No. 188; *General Motors LLC v. Thompson*, CIRA No. 191; *LEGO Juris A/S v. Abbott*, CIRA No. 193; *Ontario Physical and Health Education Association v. Jump-Aerobics Inc.*, CIRA No. 197; *Georgia-Pacific Consumer Products LP v. Walker*, CIRA No. 198; *Weekday Brands AB v. Leslie,* CIRA No. 201; *LEGO Juris A/S v. Lehmann*, CIRA No. 211; *Magna International Inc. v. Silva*, CIRA No. 212; *Georgia-Pacific Consumer Products LP v. Gaudry*, CIRA No. 213).
- A complainant who relies upon rights in an unregistered trade-mark must prove that the trade-mark was used by the complainant or its predecessor or licensor before the disputed domain name was registered (*JOBRAPIDO S.r.l. v. Langue*, CIRA No. 186; *Forest Laboratories Canada Inc. v. Netnic Corporation*, CIRA No. 187; *Chambers v. Concrete Specialists Ltd.*, CIRA No. 195; and *Alberta Foundation and Concrete Lifting Ltd. v. Concrete Specialists Ltd.*, CIRA No. 207).
- A complainant must provide evidence of the registration of a disputed domain name; unsupported allegations are not sufficient (*Luidia, Inc. v. Nirumvala*, CIRA No. 214).

B. Copyright and the Internet

1. Copyright Modernization Act—Amendments to *Copyright Act*

The federal government's Bill C-11—the *Copyright Modernization Act*, S.C. 2012 c. 20 (the "*CMA*") received royal assent in June 2012 and many of its provisions were proclaimed in force in November 2012. The stated purposes of the *CMA* include addressing the challenges and opportunities presented by the Internet, aligning Canadian copyright law with international standards, clarifying Internet service providers' liability and making the enabling of online copyright infringement itself an infringement of copyright, and ensuring that the *Copyright Act* remains

technologically neutral. The *CMA* makes a number of significant changes to the *Copyright Act* that are directly relevant to use of the Internet and related technologies. Following is a summary of some of those changes:

- **Internet Service Providers:** An Internet service provider does not infringe copyright in a work solely by acting as an intermediary providing the means (including caching for the purposes of efficiency) for the telecommunication or reproduction of the work, subject to various restrictions and requirements.
- **Hosting Service Providers:** An Internet service provider who provides digital memory (e.g., online network storage) in which another person stores a work does not, by virtue of that act alone, infringe copyright in the work, but this exception does not apply if the ISP knows of a court decision holding that the person storing the work is infringing copyright in the work.
- **Search Engines:** A provider of an information location tool (a search engine or other tool to locate information available through the Internet) that is found to have infringed copyright by reproducing a work or by communicating a work to the public by telecommunication may be subject to an injunction, but the provider is not otherwise liable for any other copyright infringement remedies (e.g., damages) if the provider acts solely for the purpose of providing the information location tool and subject to other restrictions and requirements.
- **Notice-and-Notice Regime:** A hosting service provider who receives a prescribed form of notice of alleged copyright infringement regarding materials hosted by the service provider and is paid a prescribed fee, must forward the notice to the person to whom the hosting services are provided; confirm to the claimant that the notice was forwarded (or why it was not forwarded); and retain records identifying the person to whom the hosting services are provided for six months or a year (if notified that legal proceedings have been commenced within the initial six-month period),. A hosting service provider who fails to comply with the notice-and-notice regime is subject to statutory damages between $5,000 and $10,000. The notice-and-notice regime is significantly different from the notice-and-take-down regime that applies under U.S. law. (These provisions were not proclaimed in force.)
- **Liability for Enabling Infringement:** It is an infringement of copyright to provide an Internet service primarily for the purpose of enabling acts of copyright infringement if an actual copyright infringement occurs as a result of the use of the service.
- **Expanded Fair Dealing:** The permissible purposes for the fair dealing exception to copyright infringement are expanded to include each of education, parody and satire.
- **Software—Compatibility/Interoperability:** It is not an infringement of copyright in a computer program for a person who owns or has a licence to use a copy of the computer program to reproduce and modify the computer program to make it compatible with a particular computer for the person's own use, or to reproduce it for the sole purpose of obtaining information to make the program interoperable with another program, subject to various restrictions and requirements.
- **Technological Protection Measures:** Technological protection measures ("TPMs"), also known as "digital locks", are technologies, devices or components designed to either control access to a work or to restrict certain uses of a work. A person is liable for copyright infringement damages and other remedies if the person circumvents an access control TPM; provides or offers services to the public primarily for the purpose of circumventing a TPM; or manufactures, imports, distributes, offers to sell or rent, or provides any technology, device or component that is designed or produced primarily for the purpose of circumventing a TPM or that is marketed for that purpose. There are limited and restricted exceptions to the prohibitions regarding TPMs, and limitations on remedies in certain circumstances. Additional exceptions may be added by regulation. Fair dealing is not an exception to the prohibitions regarding TPMs. Subject to limited exceptions, a person who knowingly and for commercial purposes contravenes the prohibitions regarding TPMs commits an offence and is liable to a fine of up to $1 million and imprisonment for up to five years.
- **Rights Management Information:** Rights management information is information that is attached to or embodied in a copy of a work or appears in connection with its communication to the public, and either identifies or permits the identification of the work, the copyright owner, and the terms or conditions of use of the work. A person is liable for copyright infringement damages and other remedies if the person knowingly removes or alters any rights management information in electronic form and the person knows or ought to know that doing so will facilitate or conceal an infringement of copyright in the work, or if the

person does certain acts regarding a work if the person knows or ought to know that rights management information has been removed from the work.

- **Making Available Right:** Copyright in a work now expressly includes the exclusive right to make the work available to the public by telecommunication in a way that allows a member of the public to have access to the work using pull technologies.
- **Non-Commercial User Generated Content:** It is not an infringement of copyright for an individual to use a publicly available existing work to create a new copyright protected work (commonly known as "user generated content"), to use the new work or to authorize an intermediary to disseminate the new work, subject to a number of restrictions and requirements, including: the use and dissemination of the new work are for non-commercial purposes; certain information regarding the existing work is mentioned, if reasonable to do so; the individual has a reasonable belief that the existing work itself is not infringing copyright; and the use and dissemination of the new work does not have a substantial adverse effect (financial or otherwise) on the exploitation or potential exploitation of the existing work or the market for it. The creation of non-commercial user generated content is not an exception to the rules regarding TPMs.
- **Private Copying/Time Shifting:** It is not an infringement of copyright for an individual to reproduce a lawfully obtained copyright work for the individual's private purposes or to record a broadcast program (as long as it is not part of an on-demand service) for the individual's private listening or viewing (e.g., recording a television show for later viewing), subject to various restrictions and requirements, including that the individual does not circumvent TPMs to make the reproduction.
- **Back-up Copies:** It is not an infringement of copyright for a person who owns or has a licence to use a non-infringing copy of a work to make another copy of the work solely for the person's own backup purposes, subject to various restrictions and requirements, including that the person does not circumvent TPMs to make the backup.
- **Statutory Damages:** The rules regarding statutory damages now differentiate between infringement for commercial purposes and infringement for non-commercial purposes. Statutory damages for commercial infringements are unchanged—a maximum of $20,000 for each infringed work. Statutory damages for non-commercial infringements are substantially reduced and limited—$5,000 for all non-commercial infringements of all works involved in a legal proceeding, and the defendant infringer is not liable to the plaintiff in the proceeding or any other copyright owner for statutory damages for any other infringements done for non-commercial purposes before the commencement of the legal proceeding.
- **Encryption Research:** It is not an infringement of copyright for a person to reproduce a lawfully obtained work (including a computer program) for the purposes of encryption research, subject to various restrictions and requirements.
- **Security Assessment:** It is not an infringement of copyright for a person to reproduce a work for the sole purpose of assessing the vulnerability of a computer, computer system or network or of correcting any security flaws, provided that the person has the consent of the owner or administrator of the computer, computer system or network and subject to various other restrictions and requirements.
- **Technological Processes:** It is not a copyright infringement to make a reproduction of a work if the reproduction is an essential part of a technological process to facilitate a use that is not an infringement of copyright, and the reproduction exists only for the duration of the technological process.

2. Online Music Previews Are Fair Dealing

Society of Composers, Authors and Music Publishers of Canada v. Bell Canada, 2012 SCC 36, involved judicial review of a Copyright Board decision that copyright royalties are not payable for Internet music previews. The Supreme Court of Canada affirmed the Copyright Board's decision. The court held that the fair dealing exception for purposes of "research" must be given a large and liberal interpretation applied from the perspective of the ultimate user or consumer, and included research for commercial purposes (in this case, to research and identify musical works for online purchase). The court held that the dealing was fair in light of all of the circumstances, including the use of reasonable safeguards (the previews are streamed, short and often of lesser quality than the musical works); the character of the dealing (previews are streamed to and automatically deleted from a user's computer after the preview is heard); the amount of the dealing (which the court held should be assessed based upon the proportion of the preview in relation to the musical work as a whole); and other considerations (the lack of a reasonable, efficient alternative and the fact that the purpose of previews is to increase the sale of complete musical

works). The court reasoned that the Board's decision properly balanced the purposes of the *Copyright Act* by encouraging the creation and dissemination of works while at the same time ensuring that creators are fairly rewarded.

3. Downloading is not a "Communication" Subject to SOCAN's Tariff

Entertainment Software Association v. Society of Composers, Authors and Music Publishers of Canada, 2012 SCC 34, involved judicial review of a Copyright Board decision regarding the application of SOCAN's copyright tariff for the communication of musical works to the public under *Copyright Act* s. 3(1)(f) to musical works contained in video games downloaded over the Internet. A majority of the Supreme Court of Canada set aside the Copyright Board decision on the basis that copies of musical works downloaded over the Internet (which are permanently stored on the user's computer) constitute a reproduction of the musical work (for which a reproduction royalty is payable), but do not constitute a communication of a work to the public by telecommunication under *Copyright Act* s. 3(1)(f), for which an additional, separate communication royalty is payable. The court majority held that the right to "communicate" a work to the public is a performance-based right that does not include the Internet delivery of a permanent copy of a work (which implicates a reproduction right). The court majority reasoned that this approach was consistent with a technologically neutral interpretation of the *Copyright Act* that avoids imposing an additional layer of protections and fees based solely on the method of delivery of a work to the end user. The dissenting minority of the court held that the Internet distribution of a work implicates both communication and reproduction rights, reasoning that the right to communicate a work under *Copyright Act* s. 3(1)(f) is a self-standing right that is not limited to performance activities.

4. Streaming Is a "Communication" Subject to SOCAN's Tariff

Rogers Communications Inc. v. Society of Composers, Authors and Music Publishers of Canada, 2012 SCC 35, involved judicial review of a Copyright Board decision regarding the application of SOCAN's copyright tariff for the communication of musical works to the public under *Copyright Act* s. 3(1)(f) to musical works downloaded or streamed over the Internet. The Copyright Board held that downloads (which result in a permanent copy of a work) and streams (which result in a temporary copy of a work that is automatically deleted after the work is heard) are each subject to royalties for communication to the public under s. 3(1)(f) of the *Copyright Act*. The Supreme Court of Canada set aside the Copyright Board's decision that music downloads constitute a communication to the public for the reasons set forth in *Entertainment Software Association v. Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 34. The Supreme Court of Canada upheld the Copyright Board's decision that music streams constitute a communication to the public. The court rejected the ISPs' argument that streaming is a private, point-to-point transaction based upon pull technologies initiated by a user independently of other users. The court held that the communication right is not restricted to a purely non-interactive context and it matters little whether members of the public receive a communication of the same work in the same or in different places, at the same or at different times, or at their own or the sender's initiative. The court reasoned that its approach was consistent with a technologically neutral interpretation of the *Copyright Act* that ensures the continued relevance of the communication right in an evolving technological environment.

5. No Copyright Infringement for Linking to Photographs Posted by Plaintiff

Warman v. Fourier, 2012 FC 803, involved a dispute over the alleged infringement of the plaintiff's copyright in three works—a speech, an article, and a photograph. The defendants' political discussion website reproduced copies of the speech and excerpts from the article, and included a link to the photograph as it appeared on the plaintiff's own website. The court dismissed the plaintiff's claim regarding the speech because the plaintiff commenced the lawsuit after the three-year limitation period prescribed by the *Copyright Act* expired. The court dismissed the plaintiff's claim regarding the article because the defendants did not reproduce a substantial part of the article (the reproduced excerpts were not quantitatively or qualitatively a substantial part of the original) and the reproduction was fair dealing for the purposes of news reporting protected by *Copyright Act* s. 29.2. The court dismissed the plaintiff's claim regarding the unauthorized link to the photograph because the plaintiff authorized the defendants' communication of the photograph by telecommunication by posting a copy of the photograph on the plaintiff's publicly available website and the plaintiff could remove the photograph from his website if he did not wish to have other sites link to the photograph.

6. Damages for Copyright Infringement

Adobe Systems Inc. v. Thompson, 2012 FC 1219, involved claims by three software vendors that the defendant infringed the vendors' copyright in various software products by selling counterfeit copies of the software through the popular Kijiji and Craigslist websites. The plaintiffs applied for summary judgment. The defendant denied any wrongdoing and claimed that the plaintiffs were to blame because they failed to include protective measures in their software. The court held that the defendant had engaged in egregious infringing conduct that required a clear deterrent message to the defendant and anyone else of like mind. The court issued an injunction prohibiting further infringement by the defendant and awarded maximum statutory damages ($20,000 for each software product infringed), modest punitive damages ($15,000 to each plaintiff), pre-judgment and post-judgment interest and costs on a solicitor-client basis.

7. Enforcement of U.S. Copyright Infringement Judgment

Blizzard Entertainment, Inc. v. Simpson, 2012 ONSC 4312, involved an application by the plaintiff to have a default judgment of a U.S. court recognized and enforced in Ontario. The U.S. court order granted an injunction and damages against the defendant for hacking the popular StarCraft online computer game. The defendant, an Ontario resident, was properly served with notice of the U.S. lawsuit but did not defend or otherwise respond to the lawsuit. The U.S. court issued default judgment against the defendant, but he did not attempt to appeal or otherwise challenge the judgment. The defendant opposed the Ontario court's enforcement of the U.S. judgment, arguing that the judgment was based on evidence that the plaintiff obtained improperly from the defendant's website in breach of the website terms of use, which expressly prohibited use of the website by the plaintiff and other video game companies. The court rejected the defendant's argument as being "untenable" and not an applicable defence to enforcement of a foreign judgment. The court held that the U.S. judgment should be recognized and enforced because the U.S. court properly assumed jurisdiction over the defendant and there were no applicable defences of fraud, breach of natural justice or public policy upon which the court could refuse to enforce the judgment. The court also held that the injunctive relief ordered by the U.S. court was sufficiently clear and specific to be enforceable in Canada.

C. Contracts and the Internet

1. Email Contract for Sale of Land Satisfies Statute of Frauds

Druet v. Girouard, 2012 NBCA 40, involved a dispute relating to negotiations for the sale of a residential condominium. The negotiations were conducted by a series of seven emails between non-commercial parties. The defendant refused to complete the transaction and argued that the emails did not constitute a binding contract or satisfy the formalities required by the *Statute of Frauds*. A motions judge held that the emails constituted a binding contract because they set forth all of the essential terms of the agreement and satisfied the writing and signature requirements of the *Statute of Frauds*. On appeal, the Court of Appeal held that the alleged agreement was unenforceable because the parties did not have the requisite intention to create a binding agreement. The Court of Appeal held that the emails were merely non-binding preliminary negotiations, noting that the buyer had not inspected the condominium or obtained details of the mortgage the buyer was to assume, and the buyer had offered to have a formal agreement of purchase and sale prepared for the vendor's review. The Court of Appeal confirmed that emails can satisfy the writing requirement of the *Statute of Frauds*, and considered but did not determine whether email signatures can satisfy the signature requirement of the *Statute of Frauds*.

2. Exclusion Clause in Click-Through Contract

Garofoli v. Air Canada Vacations, 2012 ONSC 4698, involved a dispute relating to the plaintiffs' unsatisfactory vacation at an all-inclusive resort arranged by the defendant tour operator. The plaintiffs booked a tour package online through a travel agency website. The plaintiffs sued the tour operator for damages. The tour operator raised a number of defences, including an exclusion of liability clause contained in the tour package terms and conditions, which the plaintiffs had to "click through" when they booked the vacation. A small claims court trial judge granted judgment for the plaintiffs on the basis that the exclusionary clause was not enforceable because it was inconsistent with other provisions of the tour package terms and conditions. On appeal, the Ontario Superior Court reversed the trial judge's decision and dismissed the plaintiffs' claims on the basis that the exclusionary clause was not ambiguous or contradictory with other provisions of the tour package terms and conditions, and the plaintiffs were bound by the exclusionary clause because it was brought to their attention by the "click through" process.

D. Torts and the Internet

1. Trespass to Chattels

Insurance Corp. of British Columbia v. Canadian Office and Professional Employees Union, Local 378, 2012 BCSC 1244, involved a dispute over job action by unionized ICBC employees in connection with a collective bargaining dispute with ICBC. At the direction of the union, its members replaced the email signature prescribed by ICBC with a signature that criticized ICBC and the B.C. government and provided a link to the union website. ICBC sued the union and its members and applied for an interlocutory injunction restraining union members from changing the standard ICBC email signature. The court granted an injunction on the basis that: (a) there was an arguable case that unauthorized changes to the email signature constituted a conversion of ICBC's interest in the email correspondence, which should be treated as the equivalent of the postal (paper-based) mail that it replaced; and (b) the balance of convenience favoured granting an injunction. The court rejected ICBC's claims that the job action amounted to passing-off, interference with contractual relations and conspiracy.

2. Invasion of Privacy

Jones v. Tsige, 2012 ONCA 32, involved a dispute over the defendant's unauthorized access to the plaintiff's banking records. The defendant was a bank employee who, contrary to the bank's policy, looked at the plaintiff's bank records at least 174 times over a four-year period. The plaintiff sued the defendant for invasion of privacy. The trial judge dismissed the plaintiff's claims on the basis that Ontario law did not recognize a tort of invasion of privacy. The Ontario Court of Appeal granted the plaintiff's appeal on the basis that Ontario common law recognized a common law cause of action for invasion of privacy involving intrusion upon seclusion. The court reasoned that technological changes (the Internet and digital technology) posed novel threats to the right of privacy that had been protected for hundreds of years by the common law through various causes of action, and the common law could evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. The court identified the elements of an action for intrusion upon seclusion as follows: (a) the defendant's conduct must be intentional or reckless; (b) the defendant must without lawful justification invade, physically or otherwise, the privacy of the plaintiff or his private affairs or concerns; and (c) a reasonable person would regard the invasion as highly offensive, causing distress, humiliation, or anguish. The court held that proof of economic harm is not required, and that damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum in the range of up to $20,000. The court granted judgment for the plaintiff and awarded damages in the amount of $10,000.

E. Privacy and the Internet

1. Reasonable Expectation of Privacy in Work Computer

R. v. Cole, 2012 SCC 53, involved a criminal prosecution of a high-school teacher for possession of child pornography based upon photographs found on a work-issued laptop computer that the accused was permitted to use for incidental personal purposes. A school policy warned computer users not to expect privacy in computer files. While performing maintenance services on the computer, a school technician discovered child pornography, notified the school principal, and copied the offending files to a disc. School board technicians also copied the files to another disc. The laptop and discs were handed over to the police, who without a warrant reviewed the laptop and discs and made a mirror image copy of the laptop hard drive. The trial judge excluded all of the computer material from evidence on the basis that the police search of the laptop was an unreasonable search and seizure in violation of the accused's *Charter* rights. The summary conviction appeal court reversed the decision, and the Court of Appeal then reaffirmed the trial judge's decision other than with respect to the materials copied by the school technicians. A majority of the Supreme Court of Canada held that the warrantless police search of the laptop was an infringement of the accused's *Charter* right to be free from unreasonable search and seizure, but nevertheless concluded that the computer materials should not have been excluded from evidence because their admission would not bring the administration of justice into disrepute. The court majority held that Canadians may reasonably expect privacy in the information contained on computers that they reasonably use for personal purposes, whether in the workplace or at home. The court majority reasoned that all of the circumstances must be considered to determine whether privacy is a reasonable expectation in a particular situation, and that ownership of a computer and workplace policies and practices warning against privacy were relevant considerations but not determinative. The court majority reasoned that Internet-connected devices contain data that is meaningful, intimate and organically connected to the user's biographical core and falls at the very heart of the informational privacy protected by s. 8 of the *Charter*. The court

majority held that operational realities, such as workplace policies and practices, may diminish, but do not remove entirely, an individual's expectation of privacy in a work computer, and a reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy protected by the *Charter*. The court majority held that while the school principal and school board had a lawful right to seize the laptop and inform the police, they could not give the police a right to search the laptop without a warrant.

2. Reasonable Limits on Internet Anonymity

R. v. Ward, 2012 ONCA 660, involved an appeal by the accused from criminal convictions for accessing and possessing child pornography. The police, in the course of a child pornography investigation, sought the name and address of a customer from a Canadian Internet service provider ("ISP") pursuant to s. 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*, which provides that an organization may voluntarily disclose an individual's personal information without the individual's knowledge or consent if the disclosure is made to a government institution for the purpose of a law enforcement investigation. The ISP voluntarily chose to cooperate with the police and provided the appellant's name and address. The police used that information to obtain a search warrant for the appellant's residence and computer, and discovered child pornography during the search. At trial, the appellant defended on the basis that the search violated his *Charter* rights and the resulting evidence should be excluded. The appellant argued that he had a reasonable expectation of privacy in his subscriber information held by the ISP and that the ISP's voluntary disclosure of that information to the police violated the appellant's right to be free from unreasonable search and seizure. The trial court convicted the appellant, and the appellant appealed. The Court of Appeal characterized the appellant's privacy claim as an assertion of "a reasonable expectation of anonymity when on the Internet". The court held that in light of all of the circumstances, including the nature of the information requested by the police and the nature of the crimes being investigated, a reasonably informed person would accept that it was reasonable for the ISP to cooperate with the police and voluntarily disclose the appellant's subscriber information to the police, and therefore the appellant's privacy claim in the face of the police request was not objectively reasonable. The court reasoned that its view was reinforced by the ISP's service agreement (which expressly provided that the ISP reserved the right to disclose information in response to governmental requests and to fully cooperate with law enforcement agencies) and the ISP's acceptable use policy (which prohibited the transmission of child pornography). For those reasons, the court concluded that the ISP's disclosure of the appellant's subscriber information to the police did not violate the appellant's *Charter* right to a reasonable expectation of privacy in respect of the appellant's limited subscriber information held by the ISP. The court cautioned that all circumstances must be considered in determining whether a reasonable expectation of privacy has been violated, and that different circumstances (including disclosure of more detailed information by an ISP or the investigation of different crimes) might lead to different results.

3. Federal Privacy Commissioner Investigates Facebook

In April 2012, the Office of the Privacy Commissioner of Canada ("OPC") issued findings in three investigations involving Facebook (PIPEDA Reports of Findings #2011-005, #2011-006 and #2012-002). Two complaints—involving Facebook's identity authentication practices and alleged sharing of information with organizations hosting social plug-ins—were determined to be not well-founded. A third complaint—involving Facebook's friend suggestion emails to non-members—was determined to be well-founded and resolved. The friend suggestion email complaint related to Facebook's practice of encouraging members to send invitations to non-members and automatically including in those invitations friend suggestions generated by Facebook using the non-members' email addresses. The OPC acknowledged that Facebook could reasonably rely on its members to obtain a non-member's consent before sending an invitation to the non-member. Facebook expressly required its members to do so. However, Facebook was obligated to obtain the non-member's consent before using the non-member's email address to generate friend suggestions. The OPC found that the required consent could be obtained using an appropriate opt-out procedure (including clear and adequate notice of the use of email addresses to generate friend suggestions and a conspicuous, convenient and user-friendly opt-out procedure). Facebook implemented the recommended opt-out procedure during the course of the investigation.

4. Federal Privacy Commissioner Issues Guidelines for Online Behavioural Advertising

In June 2012, the Office of the Privacy Commissioner of Canada issued updated guidelines entitled "*Privacy and Online Behavioural Advertising*" (www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.asp) to help organizations involved in online behavioural advertising ensure that their online behavioural advertising practices comply with Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA). Online behavioural advertising often involves sending targeted advertisements based upon an individual's Internet activities, including

purchasing patterns and search queries. The guidelines take the position that information involved in online tracking and targeting for behavioural advertising to individuals generally constitutes personal information. The guidelines remind that PIPEDA requires an individual's informed consent to the collection, use or disclosure of personal information, and that the purpose for which an individual's personal information is to be collected, used or disclosed must be explained in a clear and transparent manner. The guidelines acknowledge that opt-out consent for online behavioural advertising may be appropriate and reasonable in certain circumstances, including appropriate disclosure and transparency, limited data collection, easy opt-out mechanisms, immediate implementation of opt-out requests, and timely destruction of collected information. The guidelines also indicate that, as a best practice, organizations should avoid tracking children and tracking websites aimed at children. The Office of the Privacy Commissioner of Canada also issued the *Policy Position on Online Behavioural Advertising* (www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp).

5. Privacy Commissioners Issue Guidelines for Mobile Applications

In October 2012, the Offices of the Privacy Commissioners of Canada, Alberta, and British Columbia issued a guidance document entitled "*Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*" to provide guidance for developers of mobile applications ("apps") to ensure compliance with Canadian privacy laws. The guidelines remind that Canadian privacy laws require businesses (including mobile app developers) to balance innovation and entrepreneurialism with effective privacy protection. The guidelines note that Canadians are concerned about privacy, and mobile apps that take privacy seriously can have a competitive advantage. The guidelines recommend: (a) organizations should establish and implement appropriate policies and practices for privacy protection, and address privacy protection in all business arrangements and contracts; (b) app users should be informed, in a clear, understandable, and timely manner, about what is being done with their personal information; (c) apps should collect only the personal information (including device-unique identifiers) that is reasonably required for the legitimate purposes of the app, and should allow users to opt-out of the collection of personal information, and collected personal information about a user should be securely stored (using encryption) on the app and in supporting infrastructure and automatically deleted when the user deactivates and deletes the app; (d) apps should display privacy notifications that are effective and suitable for the small screen of a mobile device (e.g., using layering, a privacy dashboard, and visual cues); and (e) apps should display appropriate privacy notices in a timely way, before the app is downloaded, when the app is used for the first time, and in real time whenever the app collects personal information, to ensure that the user's consent remains meaningful and relevant. Similar guidance may be found in the U.S. Federal Trade Commission's guidance document entitled "*Marketing Your Mobile App—Get It Right from the Start*" (www.ftc.gov/opa/2012/09/mobileapps.shtm), published in August 2012.

6. Ontario Privacy Commissioner Issues Warning About Social Media

In April 2012, the Office of the Information and Privacy Commissioner of Ontario updated its educational booklet entitled "*Reference Check: Is Your Boss Watching? The New World of Social Media: Privacy and Your Facebook Profile*" (www.ipc.on.ca/images/Resources/facebook-refcheck.pdf). The booklet cautions employees and job-seekers of the potential risks associated with indiscreet social media postings and explains the use of social media by employers when conducting background checks. The booklet advises users of Facebook and other social media sites to post information with their eyes wide open, considering the risks to their current and future employment prospects. The booklet also suggests strategies to mitigate the risks associated with the use of social media. Related guidance for employers may be found in *Guidelines for Social Media Background Checks* issued by the Office of the Information and Privacy Commissioner for British Columbia (www.oipc.bc.ca/guidance-documents/1454) and by the Office of the Information and Privacy Commissioner for Alberta (www.oipc.ab.ca/downloads/documentloader.ashx?id=2933).

F. Regulatory and Criminal Matters

1. Canada's Anti-spam and Online Fraud Act

Canada's anti-spam and online fraud act (Bill C-28, commonly known as "CASL") creates a comprehensive regime of offences, enforcement mechanisms, and potentially severe penalties (including personal liability for corporate directors and officers) designed to prohibit unsolicited or misleading commercial electronic messages ("CEMs") and deter other forms of online fraud such as identity theft, phishing, and spyware. CASL has not yet been proclaimed in force because required regulations have not been finalized.

CASL gives the Canadian Radio-television and Telecommunications Commission ("CRTC") regulatory and

enforcement authority regarding CEMs and other matters. In March 2012, CRTC issued its *Electronic Commerce Protection Regulations* (SOR/2012-36) specifying various requirements for compliance with CASL's information disclosure and consent requirements, including the information to be disclosed when requesting consent to receive a CEM and the form and content of a CEM. Following is a summary of the regulations as they relate to CEMs:

- **Request for Consent:** A request for consent to receive a CEM may be made orally or in writing. A request for consent to receive a CEM must include a statement identifying the person seeking the consent and the person on whose behalf the consent is sought (if applicable); the business name and actual name (if different) of the person seeking the consent and the person on whose behalf the consent is sought (if applicable); contact information (mailing address and either telephone number, email address, or web address) for each of them (if applicable); and a statement indicating that the person whose consent is sought can withdraw the consent.
- **CEM Content:** A CEM must clearly and prominently identify the person sending the CEM and the person on whose behalf the CEM is sent (if applicable); and set out the business name and actual name (if different) of both the actual sender of the CEM and the person on whose behalf the CEM is sent (if applicable); and contact information (mailing address and either telephone number, email address, or web address) for each of them (if applicable).
- **CEM Form:** If it is not practicable to include the prescribed information and the required unsubscribe mechanism in a CEM, the information may be posted on a website that is readily accessible by the CEM recipient by means of a clear and prominent link in the CEM.
- **Unsubscribe Mechanism:** The required unsubscribe mechanism must be able to be readily performed.

In October 2012, CRTC issued two information bulletins—Guidelines on the Interpretation of the Electronic Commerce Protection Regulations (CRTC 2012-548) and Guidelines on the use of toggling as a means of obtaining express consent under Canada's anti-spam legislation (CRTC 2012-549). The bulletins provide guidance regarding the interpretation and application of the CRTC regulations and compliance with CASL's information disclosure, consent, and unsubscribe requirements. Following is a summary of the key elements of the guidelines as they relate to CEMs:

- **Identification of Sender:** If a CEM is sent on behalf of multiple persons, such as affiliated organizations, then each of those persons must be identified. There is no obligation to identify intermediaries (neither a person sending a CEM nor a person on whose behalf a CEM is sent) who facilitate the distribution of a CEM but have no role in its content or choice of recipients.
- **Mailing Address:** The mailing address of a sender (which must be disclosed in a CEM) consists of the sender's valid, current street (civic) address, postal box address, rural route address, or general delivery address, and must be valid for a minimum of 60 days after the CEM has been sent.
- **Unsubscribe Mechanism:** An unsubscribe mechanism must be "readily performed", which means that it must be accessible "without difficulty or delay" and should be "simple, quick and easy" for a consumer to use. Examples of a "readily performed" unsubscribe mechanism are a link in an email or a SMS message that takes the user to a website where the user can unsubscribe from receiving CEMs from the sender, or the ability to respond to a SMS message with the word "STOP" or "unsubscribe" that unsubscribes the person from receiving further CEMs from the sender.
- **Separate Consents:** A person seeking consent for activities regulated by CASL must seek a separate consent for each kind of activity, and a person from whom consent is sought must be able to consent to some activities and refuse to consent to other activities. It is not necessary for consent to be sought separately for each instance of a regulated activity, as long as the initial consent request complies with the requirements of CASL.
- **Consent Requests:** Requests for consent to activities regulated by CASL must be clearly identified and must not be subsumed in, or bundled with, requests for other consents (e.g., consents to terms and conditions of use or sale). For example, consents to regulated activities may be obtained by using a separate tick-box or icon (which must be proactively ticked or clicked) to indicate consent to each kind of activity.
- **Consent Obtained Orally:** A person relying on an oral consent may discharge the onus of demonstrating consent if the oral consent can be verified by an independent third party or by a complete and unedited audio recording of the oral consent retained by the person seeking consent or a client of the person seeking consent. A person may request and obtain oral consent in situations where information is collected over the

phone (e.g., call centres), or a person may give consent when the person uses a product or service (e.g., point of sale purchases).

- **Consent Obtained in Writing:** Written consent includes both paper writing and electronic forms of writing. An electronic form of writing must permit the recorded information to be "subsequently verified". For example, acceptable consent in writing includes checking a box on a web page to indicate consent (where a record of the date, time, purpose, and manner of the consent is stored in a database) and filling out a consent form at a point of purchase.
- **Opt-In Toggling:** Express consent to activities regulated by CASL can be obtained through opt-in consent mechanisms (such as checking a box or typing an email address into a designated field to indicate consent) because they enable a person to positively and explicitly express their consent.
- **Opt-Out Toggling:** Express consent to activities regulated by CASL cannot be obtained through opt-out consent mechanisms. Accordingly, opt-out toggling (the presentation of a consent form with a default toggling state that assumes consent) cannot be used as a means of obtaining express consent under CASL.
- **No CEM to Request Consent:** An unsolicited email, text message, or other form of CEM cannot be used to request express consent.
- **Confirmation of Consent:** After a person gives express consent, confirmation of receipt of the consent should be sent to the person.

On January 5, 2013, Industry Canada published revised draft regulations for CASL and substantial commentary. The draft regulations define some key terms and concepts (family relationship, personal relationship, and membership in a club, association or voluntary organization) contained in CASL, specify exemptions to the restrictions regarding CEMs, and specify conditions for the use of a consent to receive CEMs from unknown senders. Industry Canada first published draft regulations in 2011, and the revised draft regulations represent the government's response to feedback from various stakeholders. The draft regulations are available at www.gazette.gc.ca/rp-pr/p1/2013/2013-01-05/html/reg1-eng.html.

2. ISPs are not Regulated Broadcasters

Reference re Broadcasting Act, 2012 SCC 4, involved an application by the Canadian Radio-television and Telecommunications Commission to determine whether Internet service providers ("ISPs") carry on "broadcasting undertakings" subject to the *Broadcasting Act* when they provide their customers with Internet access to third party broadcasting services. The Federal Court of Appeal 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. On appeal, the Supreme Court of Canada unanimously affirmed the Federal Court of Appeal's decision, reasoning that the terms "broadcasting" and "broadcasting undertaking", interpreted in the context of the language and purposes of the *Broadcasting Act*, are not meant to capture entities that merely provide a mode of transmission, and do not include ISPs who take no part in the selection, origination or packaging of content but merely provide access through the Internet to third party broadcasting content requested by end-users.

G. Internet Defamation

1. Plaintiff Anonymity in Cyberbullying Cases

A.B. v. Bragg Communications Inc., 2012 SCC 46, involved cyberbullying of the applicant, a teenage girl. The applicant sought an order requiring an Internet service provider to disclose the identity of the persons who used an IP address to publish a fake Facebook page of her, so that she could identify potential defendants for a defamation action. A chambers judge rejected the applicant's request for anonymity and a publication ban regarding the content of the Facebook page. The Nova Scotia Court of Appeal dismissed the applicant's appeal on the basis that her reluctance to have personal and potentially embarrassing information disclosed in open court was not sufficient to override the fundamental open-court principle, and she had not discharged the onus of showing that there was real and substantial harm to her that justified restricting media access. The Supreme Court of Canada granted the applicant's appeal on the basis that privacy and the protection of children from cyberbullying were sufficiently compelling considerations to justify exceptions to the open-court principle. The court held that in cases involving cyberbullying of children a court could rely upon objectively discernable harm, based upon common sense, reason

and logic, to justify a ban on the publication of the child victim's identity. The court also held that once the girl's identity was protected there was no justification for a publication ban regarding non-identifying Facebook content.

2. Jurisdiction over Internet Defamation Claims

Breeden v. Black, 2012 SCC 19, involved a number of lawsuits for defamation commenced by a well-known business figure and former chair of a publicly traded U.S. company. The lawsuits related to a number of disparaging statements and reports that were published or posted on the website of the company and were then downloaded, read, and republished by three Canadian newspapers. The defendants applied to stay the lawsuits on the grounds that the plaintiff was a "libel tourist" and there was no real and substantial connection between the lawsuits and Ontario, or alternatively that a U.S. court was the more appropriate forum. The motions judge dismissed the defendants' application and the Ontario Court of Appeal dismissed their appeal. The Supreme Court of Canada held that the Ontario court had jurisdiction over the lawsuits based on a real and substantial connection to Ontario because the defamatory statements were read, downloaded and republished in Ontario. The court noted that it is well established that the original author of a defamatory statement may be held liable for a republication that is authorized by the author or that is a natural and probable result of the original publication. The court further held that the Ontario trial court should not decline to exercise jurisdiction over the lawsuits because the U.S. court was not a clearly more appropriate forum. The court noted that the plaintiff had undertaken not to bring a libel action in any other jurisdiction and had limited his claim to damages to his reputation in Ontario.

3. Blogging Context Considered When Assessing Defamation

Baglow v. Smith, 2012 ONCA 407, involved an acrimonious political debate on Internet blogs in which the defendant referred to the plaintiff as "one of the Taliban's more vocal supporters". The trial court granted the defendant's application for summary judgment, holding that the defendant's statement was made in the context of a political debate and that reasonable readers would not see the comment as harming the plaintiff's reputation. The Court of Appeal granted the plaintiff's appeal and directed that the matter proceed to trial. The court reasoned that the case presented important issues that "arise in the relatively novel milieu of Internet defamation in the political blogosphere" and that did not lend themselves to determination on a motion for summary judgment. The court noted that the case involved an alleged defamatory statement "made in the course of a robust and free-wheeling exchange of political views in the Internet blogging world where … arguments can be at times caustic, strident or even vulgar and insulting", and the case presented novel issues, including whether the legal considerations in determining whether a statement is or is not defamatory in those kinds of situations are different from those that apply to a statement published in traditional media.

4. Internet Publication in Jurisdiction

Nazerali v. Mitchell, 2012 BCSC 205, involved a dispute over a number of alleged defamatory articles about the plaintiff published on the deepcapture.com website. The notice of claim alleged that the articles were published, but did not expressly allege that anyone in British Columbia had read the alleged defamatory articles. The defendants applied to dismiss the action on the basis that the allegations in the notice of claim were not sufficient to give the court jurisdiction. The court agreed with the defendants that the notice of claim was deficient because it did not contain an allegation that anyone in British Columbia either downloaded or read the defamatory articles from the website. Nevertheless, the court dismissed the defendants' application and allowed the lawsuit to proceed because the affidavits filed by the plaintiff, together with the notice of claim, were sufficient to establish a good arguable case that the defamatory articles were downloaded or read by someone in British Columbia.

5. Jurisdiction Over Defamation Claims

Court v. Debaie, 2012 ABQB 640, involved a dispute between estranged family members over the defendants' defamatory postings on public portions of their Facebook pages. The plaintiffs (both resident in Alberta) commenced lawsuits in Alberta. The defendants (residents in Nova Scotia and Ontario) challenged service and jurisdiction, and alternatively applied to have the lawsuits stayed in favour of lawsuits in Nova Scotia and Ontario. The court held that the tort of defamation was committed in Alberta because the defamatory postings were published and read in Alberta, reasoning that the postings would have automatically appeared on the Facebook wall of the defendants' Facebook friends in Alberta when they signed in to Facebook, which justified an inference that the postings were read by those friends. The court refused to decline jurisdiction in favour of a lawsuit in another court, following *Breeden v. Black*, 2012 SCC 19, in reasoning that it would be unfair to the plaintiffs to prevent a lawsuit in the community where the plaintiffs' reputation was established.

6. Defamation Claims over Ratings Website

Walsh Energy Inc. v. Better Business Bureau of Ottawa-Hull Inc., 2012 ONSC 5819, involved a dispute over the defendant's ratings of the plaintiffs' businesses posted on the defendant's consumer protection website. The plaintiffs claimed that the posted "B" and "D-" ratings were unjustified and defamatory. The court held that the ratings were not defamatory, reasoning that they had to be read in the context of the website as a whole and additional reports explaining the ratings. The court further held that even if the ratings were defamatory, the defendant could rely upon defences of qualified privilege and fair comment.

7. Nominal Damages for Defamatory Email

Michie v. Guthrie-Waters, 2012 BCSC 793, involved an action for defamation based upon a number of disparaging emails sent by the defendant (the plaintiff's ex-wife) to various recipients. The court held that all but one of the emails was protected by qualified privilege. The unprotected email was sent to the writer of a magazine article that was also defamatory of the plaintiff. The court held the defendant liable for the defamatory email, but awarded damages of only $1 because the email was sent to only one person who had himself defamed the plaintiff, the email could not reasonably have adversely affected the recipient's opinion of the plaintiff and his reputation, and the plaintiff did not claim to have suffered any loss to his reputation as a result of the email.

8. Damages for Defamatory Email

2964376 Canada Inc. v. Bisaillon, 2012 ONSC 3113, involved a dispute over a defamatory email about the plaintiff that the defendant sent to her friends and colleagues. The defendant's parents had purchased a dining room set from the plaintiff's furniture store. The furniture was damaged during delivery, and the resulting dispute between the plaintiff and the defendant's parents was eventually resolved through a small claims court lawsuit. After the lawsuit, the defendant sent the defamatory email to 38 people asking that they forward the email to other persons. The email was critical of the plaintiff and its dealings with the defendant's parents. The defendant admitted that her motivation was revenge for her parents, since "truth is the best revenge", and refused to apologize. The court held that the email was defamatory, and rejected the defendant's defences of fair comment. The court awarded damages of $15,000, noting that the scope of distribution of the email was unknown because each of the 38 recipients was encouraged to send it to other persons. The court refused to award aggravated damages because the plaintiff corporation could not complain of "hurt feelings".
