CANADIAN INTERNET LAW UPDATE – 2017*

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

This paper summarizes selected developments in Canadian Internet law during 2017. Internet law is a vast area that continues to develop rapidly. Reference to current legislation, regulatory policies, guidelines and case law is essential for anyone addressing these issues in practice.

A. Trade-marks

1. Infringing Domain Name and Keyword Advertising

Vancouver Community College v. Vancouver Career College (Burnaby) Inc., 2017 BCCA 41, involved a dispute over the respondent's use of "VCC" in its Internet domain name and the use of "VCC" and "Vancouver Community College" as advertising keywords, which Vancouver Community College alleged constituted passing off and violation of its official marks. The trial court dismissed those claims (see 2015 BCSC 1470). The Court of Appeal allowed Vancouver Community College's appeal regarding the respondent's use of "VCC" in its domain name, but dismissed the appeal regarding the advertising keywords. The Court of Appeal held that the trial judge erred in applying the "first impression" test for confusion by holding that the relevant first impression occurs when an individual using an Internet search site arrives at a listed website. The Court of Appeal held that the proper question was whether there was a likelihood of confusion when the search results, displaying the respondent's "VCCollege.ca" domain name, appeared to an Internet user. The Court of Appeal held that there was a likelihood of confusion because the respondent's domain name was equally descriptive of both the respondent and Vancouver Community College and contained the "VCC" acronym long associated with Vancouver Community College. The Court of Appeal reasoned that there was nothing about the "VCCollege.ca" domain name that distinguished the owner of that name from Vancouver Community College, that the letters "ollege" added to the "VCC" acronym were "equally reminiscent" of Vancouver Community College as the respondent, and there were no words or letters that disclaimed affiliation with Vancouver Community College. The Court of Appeal affirmed the trial judge's decision that bidding on advertising keywords does not constitute passing off because bidding on keywords, by itself, does not deliver a confusing message. The Court of Appeal held that Vancouver Community College was entitled to a permanent injunction restraining the respondent from using "VCC" and "VCCollege" regarding its Internet presence. An application for leave to appeal to the Supreme Court of Canada was refused (*Vancouver Career College (Burnaby) Inc., dba Vancouver Career College, also dba CDI College, also dba Vancouver College of Art and Design also dba Eminata Group v. Vancouver Community College*, 2018 CanLII 1154 (SCC)).

2. Domain Name Dispute

Boaden Catering Ltd. v. Real Food for Real Kids Inc., 2017 ONCA 248, involved a dispute between competing catering companies over Internet domain names. Boaden registered domain names that were identical or similar to names that RFRK had used for many years. RFRK successfully challenged the domain name registrations in arbitration proceedings under the *Uniform Domain Name Dispute Resolution Policy* and the *CIRA Domain Name Dispute Resolution Policy*, and the arbitrators ordered the domain names transferred to RFRK. Boaden then commenced a lawsuit in the Ontario Superior Court for a declaration that Boaden was the lawful owner of the domain names. A motions judge dismissed Boaden's claims on the basis that Boaden had registered the domain names in bad faith for the purpose of exploiting the value of the defendant's trademarks or for illegitimate financial gain, and had engaged in unethical and deceptive conduct (see 2016 ONSC 4098). Boaden appealed and argued that the motions judge erred by failing to apply the test set out in *Black v. Molson Canada*, 2002 CanLII 49493 (ON SC), which reflects the criteria for a successful domain name dispute under the *Uniform Domain Name Dispute Resolution Policy*. The Court of Appeal rejected that argument, and

dismissed the appeal, on the basis that the motions judge had applied that test and had considered all of the evidence provided by Boaden.

3. Consumer Criticism Website

United Airlines Inc. v. Cooperstock, 2017 FC 616 and 2017 FC 617, involved a dispute over the defendant's UNTIED.com consumer criticism website that provided disgruntled customers and other website users with information about the plaintiff airline and allowed users to submit and read complaints about the plaintiff. The defendant designed the UNTIED.com website (including graphics, logos, and colours) to have a strong resemblance to the plaintiff's official website and the plaintiff's trademarks. The UNTIED.com website included a disclaimer and a pop-up dialogue box to indicate that it was not the plaintiff's website. The plaintiff sued for infringement of its trademarks and infringement of its copyright in its official website. The court held the defendant liable for trademark infringement, passing off, and depreciating the goodwill attached to the plaintiff's trademarks. The court held that the defendant used the trademarks displayed on the UNTIED.com website in connection with services (offering information and guidance to disgruntled customers) and those trademarks were likely to cause confusion. The court found that the disclaimers on the UNTIED.com website did not avoid consumer confusion, and the pop-up dialogue box did not always function. The court found that the defendant misled users of the UNTIED.com website as to the source of the services available on the website, which tarnished the plaintiff's reputation, causing harm to the plaintiff. The court held that parody and satire are not defences to trademark infringement. The court further held that the defendant had infringed the plaintiff's copyright (see discussion below). The court concluded that the plaintiff was entitled to an injunction restraining the defendant's use of the plaintiff's trademarks. The court allowed the defendant to retain the UNTIED.com domain name, but ordered that the domain name not be used in association with the same services as provided by the plaintiff. For a related case, see *Cooperstock c. United Airlines Inc.*, 2017 QCCA 44.

B. Copyright

1. Scraping Photos from Digital Marketplace

Trader v. CarGurus Inc., 2017 ONSC 1841, involved a dispute between the operators of competing digital marketplaces for new and used vehicles. Trader (the owner of autotrader.ca) provided various services to auto dealers, including taking photos of a dealer's vehicles for use in listings on the autotrader.ca site and on the dealer's own website. When CarGurus entered the Canadian market to compete with Trader, CarGurus scraped over 150,000 of those photos from dealer websites for use on the CarGurus site. Trader sued CarGurus for infringing copyright in the scraped photos and sought $98 million in statutory damages and a permanent injunction. CarGurus argued that the photos lacked the requisite originality to be protected by copyright, because the photographers were required to take the photos in accordance with Trader's standardized procedures. The court rejected that argument because the photographers exercised skill and judgment in taking the photos. CarGurus also argued that it did not infringe copyright in some of the photos because they were not actually copied and stored on CarGurus' server but rather they were "framed" (i.e., they remained on the dealer's website but were displayed on the CarGurus site). The court rejected that argument because displaying the photos on the CarGurus site constituted making the photos available to the public by telecommunication, which is an infringement of copyright by virtue of *Copyright Act* s. 2.4(1.1). CarGurus also invoked the defence of fair dealing for the purpose of research. The court accepted that the purpose of the dealing may have been for research, but held that the dealing was not "fair" because CarGurus' purpose was commercial, the photos were displayed in their entirety, the photos were widely disseminated through the Internet for the entire life of the vehicle listing, and CarGurus had alternatives to copying the photos. CarGurus also argued that it was the provider of an information location tool and was therefore protected against liability for damages by *Copyright Act* s. 41.27(1). The court rejected that argument on the basis that the defence for information location tools applied only to intermediaries that provide tools (e.g., search engines) that enable users to navigate and find information where it is located on the Internet, not to providers that gather information from the Internet and make it available to users on the provider's own website. Trader claimed statutory damages pursuant to *Copyright Act* s. 38.1(1) calculated at $500 for each infringed photo, and argued that the court did not have discretion to award a lower amount under *Copyright Act* s. 38.1(3) because the infringement did not involve "a single medium". The court rejected Trader's argument on the basis that the undefined term "medium" includes an electronic medium (i.e. a website), and that desktop and mobile applications were simply two user interfaces for accessing the CarGurus site. The court held that statutory damages of $500 for each

infringed photo would be grossly out of proportion, and exercised its discretion to reduce the statutory damages to $2 for each infringed photo, for a total of approximately $300,000. The court found that there was no bad faith on the part of CarGurus, and therefore no basis for an award of punitive damages. The court held that there was no need for a permanent injunction because CarGurus had removed all of Trader's photographs and ceased indexing dealer websites, and had undertaken to not reproduce any future Trader photos from feed providers if Trader identified those photos.

2. Consumer Criticism Website

United Airlines Inc. v. Cooperstock, 2017 FC 616 and 2017 FC 617, involved a dispute over the defendant's UNTIED.com consumer criticism website that provided disgruntled customers and other website users with information about the plaintiff airline and allowed users to submit and read complaints about the plaintiff. The defendant designed the UNTIED.com website (including graphics, logos and colours) to have a strong resemblance to the plaintiff's official website and the plaintiff's trademarks. The UNTIED.com website included a disclaimer and a pop-up dialogue box to indicate that it was not the plaintiff's website. The plaintiff sued for infringement of its trademarks and infringement of its copyright in the plaintiff's official website. The court held the defendant liable for trademark infringement, passing off and depreciating the goodwill attached to the plaintiff's trademarks (see above). The court also held that the defendant had infringed the plaintiff's copyright in the plaintiff's official website. The court found that the defendant had copied substantial parts of the plaintiff's official website, including the overall layout of the website and the plaintiff's logos and designs. The defendant asserted the defence of fair dealing for the purpose of parody. The court rejected that defence because, while the UNTIED.com website fell within the broad definition of parody, the copying was not "fair" because of the defendant's real purpose or motive (i.e., to harm the plaintiff), the substantial amount of the dealing (i.e., copying the entire home page of the plaintiff's official website), available alternatives to the dealing and the effect of the dealing (i.e., harm to the plaintiff). The court concluded that the plaintiff was entitled to an injunction restraining the defendant's use of the plaintiff's copyright works.

3. Unauthorized Use of Facebook Photographs

Saad c. Le Journal de Montréal, 2017 QCCQ 122, involved a dispute over the *Journal*'s unauthorized use of two photographs taken by the plaintiff, a professional photographer, of his friend and posted on the friend's Facebook page with a credit to the plaintiff as the photographer. The *Journal* published (in print and online) an article about the friend, and with her permission illustrated the article with the photographs taken from her Facebook page. The *Journal* did not clear copyright in the photographs and did not identify the plaintiff as the photographer. In response to a demand by the plaintiff, the *Journal* removed the photographs from its website, but refused to compensate the plaintiff for use of the photographs. The plaintiff sued for infringement of copyright and moral rights. The *Journal* argued that it was not liable for copyright infringement because it reasonably assumed that the friend had authority to permit the use of the photographs. The court rejected that argument and held that it was not reasonable for the *Journal* to rely solely on the friend's permission without contacting the plaintiff. The court noted that the *Journal* was accustomed to clearing copyright, and the plaintiff was identified in the photo credit on the friend's Facebook page. The *Journal* also argued that its use of the photographs was fair dealing for the purpose of news reporting. The court rejected that argument because the *Journal* did not comply with the mandatory attribution requirements (i.e., identification of the source and photographer). The court held that the *Journal* infringed the plaintiff's copyright and moral rights in the photographs, and awarded the plaintiff statutory damages totalling $2,000. See also *Jomphe (Karjessy) c. Société St-Jean-Baptiste de Montréal*, 2017 QCCQ 7303.

4. Notice and Notice Regime – Order for Disclosure of Subscriber Information

Voltage Pictures, LLC v. John Doe, 2017 FCA 97, involved a proposed reverse class proceeding against unknown defendants engaged in illegal Internet sharing of the plaintiffs' copyright films. The plaintiffs brought a motion under the "notice and notice" regime set out in *Copyright Act* ss. 41.25 and 41.26 for an order that Rogers Communications, a non-party Internet service provider, disclose contact and personal information of subscribers associated with identified Internet protocol addresses, so that the plaintiffs could name the subscribers as defendants in the class proceeding. The trial court (2016 FC 881) ordered Rogers to disclose the subscribers' names and addresses, but only after the plaintiffs paid Rogers' fee (calculated at $100 per hour) for the time spent to assemble the subscriber information. The plaintiffs appealed and argued that the trial judge erred in ordering payment of Rogers' fee. The Court of Appeal granted the appeal. The Court of

Appeal held that *Copyright Act* s. 41.26(1) requires an Internet service provider to "maintain records in a manner and form that allows it to identify suspected infringers, to locate the relevant records, to identify the suspected infringers, to verify the identification work it has done (if necessary), to send the notices to the suspected infringers and the copyright owner, to translate the records (if necessary) into a manner and form that allows them both to be disclosed promptly and to be used by copyright owners and later the courts to determine the identity of the suspected infringers, and, finally, to keep the records ready for prompt disclosure" (at para. 40). The Court of Appeal further held that, in the absence of a regulation specifying applicable fees, *Copyright Act* s. 41.26(2) precludes payment of any fee to an Internet service provider for the work required to comply with *Copyright Act* s. 41.26(1). The Court of Appeal held that the notice and notice regime does not displace the common law *Norwich* disclosure order process, which continues to govern an Internet service provider's disclosure of retained records. The Court of Appeal noted that it is reasonable for an Internet service provider to insist that a plaintiff obtain a *Norwich* disclosure order to protect the Internet service provider against aggrieved customers whose information is disclosed. The Court of Appeal held that a *Norwich* disclosure order could require payment of the Internet service provider's fee for the costs associated with the act of disclosure, but those fees could not include the work required to comply with the record collection obligations imposed by *Copyright Act* s. 41.26(1). The Court of Appeal held that the burden was on an Internet service provider to prove its costs of disclosure that should be compensated, and that Rogers had failed to adduce sufficient evidence to satisfy that burden. The Court of Appeal concluded that Rogers was not entitled to any fee for compliance with the disclosure order. The Supreme Court of Canada granted Rogers' application for leave to appeal (2017 CanLII 78701).

C. Electronic Transactions

1. Social Media Terms of Use

Douez v. Facebook, Inc., 2017 SCC 33, involved a dispute over the validity and enforceability of a forum selection clause in Facebook's Terms of Use, which every user must click to accept in order to use Facebook's social network. A majority of the Supreme Court of Canada, in a three-one-three split decision, held the clause to be unenforceable and allowed the appeal (see discussion below). Six members of the court rejected Douez's argument that the clause was not enforceable because it conflicted with Facebook's assurance that it strives to respect local law, and because consumers' attention was not drawn to the clause during the online contract formation process. Karakatsanis, Wagner, and Gascon JJ.A. noted that the *Electronic Transactions Act* (British Columbia) specifically permits contractual offer and acceptance to occur in an electronic form through "clicking" online. McLachlin C.J.C. and Côté and Moldaver JJ.A. (dissenting) reasoned that the *Electronic Transactions Act* codifies the common law set out in *Rudder v. Microsoft Corp.*, 1999 CanLII 14923 (ON SC), and establishes that an enforceable contract may be formed by clicking an appropriately designated online icon.

2. Email Acknowledgment of Liability

Johal v. Nordio, 2017 BCSC 1129, involved a dispute over a debt secured by a promissory note. The plaintiff sued to enforce the promissory note. The defendant argued that the plaintiff's claims were statute barred by the *Limitation Act* (British Columbia). The plaintiff argued that the limitation period had not expired because the defendant had sent an email acknowledging the debt. The defendant did not deny sending the email, which included, at the bottom, the defendant's name, corporate position and contact information. The court held that the email constituted a signed, written acknowledgment of liability as required by *Limitation Act* s. 24(1). The court rejected the defendant's argument that the *Electronic Transactions Act* (British Columbia) definition of "electronic signature" required something more akin to a digital signature. The court reasoned that, in the context of an email, the "electronic signature" definition focuses on "whether the email sender intended to create a signature to identify him/herself as its composer and sender". The court concluded that the email satisfied the writing and signature requirements of the *Limitation Act* because the defendant's name and additional information at the bottom of the email was electronic information that was created or adopted by the defendant to sign the email and was attached to the email.

3. Email Acknowledgment of Liability

Embee Diamond Technologies Inc. v. I.D.H. Diamonds NV, 2017 SKCA 79 and 2017 SKQB 79, involved a dispute over a debt owed by the defendant for the purchase of diamonds from the plaintiff. The defendant

argued that the plaintiff's claims were statute barred by *The Limitations Act* (Sask.). The plaintiff argued that the limitation period was extended because the defendant acknowledged the debt in a series of emails between the parties. *The Limitations Act* provides that an acknowledgment "must be in writing and must be signed by the person making it". The chambers judge applied *The Electronic Information and Documents Act, 2000* (Sask.) and common law principles to hold that the emails were in "writing" and "signed" within the meaning of *The Limitations Act*. The chambers judge reasoned that *The Electronic Information and Documents Act* supplements, but does not replace, the common law approach to signatures, which permits recognition of electronic signatures and other deviations from "wet ink" signatures. The chambers judge held that the emails included electronic information (e.g., the sender's name and address at bottom of the email or a scanned handwritten signature) that was created or adopted to sign the email. The chambers judge reasoned that the use of designated, digital signatures on some emails did not disavow the contents of emails with other forms of electronic signature. The Court of Appeal dismissed an appeal from the decision on the basis that the chambers judge did not err in the interpretation and application of *The Electronic Information and Documents Act, 2000* or in the identification and application of relevant common law principles.

4. Electronic Waiver and Release

Quilichini v. Wilson's Greenhouse & Garden Centre Ltd., 2017 SKQB 10, involved a lawsuit for compensation for bodily injuries suffered by the plaintiff while participating in go-kart racing at a track operated by one of the defendants. The plaintiff alleged that he crashed his go-kart into a barrier because the go-kart was defective. Before the plaintiff participated in the races, he completed a kiosk-based registration process in which he clicked through a series of electronic pages on a computer screen and clicked an "I agree" icon on an electronic waiver and release presented on a computer screen. The waiver and release included spaces for wet ink signatures by the participant and the racetrack staff. The defendants applied for summary judgment dismissing the plaintiff's lawsuit on the basis that the waiver and release precluded all claims. The court held that the waiver and release were binding on the plaintiff. The court referenced *The Electronic Information and Documents Act, 2000* (Sask.), which expressly confirms that an agreement to contractual terms may be expressed by touching or clicking on an appropriately designated icon or place on a computer screen. The court reasoned that the availability of an alternative method of signing the waiver and release (i.e., wet ink signatures on paper) did not invalidate the plaintiff's electronic acceptance of the waiver and release. The court dismissed the lawsuit on the basis that the waiver and release was a full defence to all of the plaintiff's claims.

D. Privacy and Personal Information Protection

1. Proposed Class Action for Breach of Privacy

Douez v. Facebook, Inc., 2017 SCC 33, involved an application for certification of a class proceeding against Facebook on behalf of approximately 1.8 million British Columbia residents whose name and likeness were used in Facebook's "Sponsored Stories" advertising program in alleged violation of the *Privacy Act* (British Columbia). Facebook challenged the British Columbia court's jurisdiction on the basis that the Facebook Terms of Use, which every user must click to accept in order to use Facebook's social network, included a choice of law and forum selection clause requiring disputes be resolved in California courts according to California law.

The chambers judge rejected Facebook's challenge to the court's jurisdiction primarily on the basis that the *Privacy Act* gave the British Columbia Supreme Court exclusive jurisdiction to hear claims in respect of the statutory privacy tort, and that if the court declined jurisdiction the plaintiff would have no other forum to bring that claim. The chambers judge certified the class proceeding. Facebook appealed.

The Court of Appeal allowed the appeal on the basis that the chambers judge erred in interpreting the *Privacy Act*. The Court of Appeal held that the *Privacy Act* did not exclude the jurisdiction of foreign courts to consider *Privacy Act* claims and was not intended to override a contractual forum selection clause. The Court of Appeal further held that the plaintiff had not shown strong cause to not enforce the contractual forum selection clause. The Court of Appeal concluded that the forum selection clause should be enforced and the action stayed. Douez appealed.

The Supreme Court of Canada, in a three-one-three split decision, held the forum selection clause to be unenforceable and allowed the appeal. The entire court agreed that the enforceability of the forum selection clause ought to be determined according to the common law *Pompey* test, which requires the court to first

determine whether the clause is "valid, clear and applicable" based on ordinary contract law principles, and then determine whether the party seeking to avoid enforcement of the clause has shown "strong cause" why the clause should not be enforced. However, the court was divided over how the *Pompey* test was to be applied to a forum selection clause in a consumer contract of adhesion.

Karakatsanis, Wagner, and Gascon JJ.A. held that the forum selection clause was valid and applicable, and that the *Privacy Act* did not override the forum selection clause. They further held that the strong cause component of the *Pompey* test requires the court to consider all of the circumstances of the particular case, which in a consumer contract context include public policy considerations regarding the unequal bargaining power of the parties and the nature of the rights that a consumer relinquishes under the contract without any opportunity to negotiate. They concluded that Douez had established strong cause – the grossly uneven bargaining power between the parties to a consumer contact of adhesion, the importance of having a local court adjudicate a statutory cause of action implicating quasi-constitutional privacy rights, and other secondary factors (interests of justice, comparative convenience, and expense) – not to enforce the forum selection clause.

Abella J., in a concurring judgment, held that it was contrary to public policy to enforce the forum selection clause because the *Privacy Act* gives the British Columbia Supreme Court exclusive jurisdiction to hear claims in respect of the statutory privacy tort. Abella J. further held that the doctrine of unconscionability applied to render the forum selection clause unenforceable because of the grossly uneven bargaining power of the parties to a contract of adhesion (based in part on the fact that consumers have no meaningful choice as to whether to accept the Facebook Terms of Use given Facebook's "undisputed indispensability to online conversations") and the unfair and overwhelming procedural and potentially substantive benefit to Facebook of requiring disputes to be adjudicated in California courts.

McLachlin C.J.C. and Côté and Moldaver JJ.A., in a dissenting judgment, would have dismissed the appeal on the basis that the forum selection clause was valid and enforceable, and Douez had not shown strong cause for not enforcing the clause. They held that the *Privacy Act* did not override the forum selection clause. They further held that applying the strong cause test in a nuanced manner to consider a consumer's lack of bargaining power would overturn previous court decisions applying the *Pompey* test and substitute new and different principles that would introduce unnecessary and unprincipled uncertainty. They noted that the British Columbia Legislature had chosen not to enact legislation prohibiting the enforcement of forum selection clauses in consumer contracts.

2. PIPEDA Applies to Foreign Websites

A.T. v. Globe24h.com, 2017 FC 114, involved an application for damages and a corrective order under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) against the operator of the Romanian-based Globe24h.com website that republished and enabled searches of publicly available Canadian court and tribunal decisions containing personal information, and charged a fee for expedited removal of the personal information from the website. The Privacy Commissioner of Canada investigated and found that the Globe24h.com website collected, used and disclosed personal information in violation of *PIPEDA* (see *Complaints against Globe24h.com*, 2015 CanLII 33260 (PCC)). The applicant, a Canadian resident whose information was published on the Globe24h.com website, applied to court for damages and a corrective order against the Globe24h.com website operator. The operator did not respond to or participate in the court proceeding. The court concluded that the Globe24h.com website was a profit-making scheme to exploit the online publication of Canadian court and tribunal decisions containing personal information. The court held that *PIPEDA* applied to the Globe24h.com website because there was a "real and substantial link" between the website and Canada – the website republished Canadian court and tribunal decisions, directly targeted Canadians, and had a direct impact on Canadians – and comity did not require the court to refrain from exercising jurisdiction. The court held that the Globe24h.com website collected, used, and disclosed personal information in the course of commercial activities, and that those activities were not exclusively journalistic in nature. The court held that it had jurisdiction to issue a corrective order against the Globe24h.com website operator in Romania pursuant to *PIPEDA* s. 16(a), and issued a broad order requiring the operator to remove all Canadian court and tribunal decisions containing personal information from the Globe24h.com website and refrain from further copying and republishing of Canadian court and tribunal decisions containing personal information. The court awarded the applicant $5,000 damages because the Globe24h.com website

operator commercially benefited from the unlawful use of personal information, and acted in bad faith by failing to take responsibility and rectify the problem.

E. Internet Defamation

1. Limitation Period for Defamatory Newspaper Articles

John v. Ballingall, 2017 ONCA 579, involved a dispute over an alleged defamatory article published on the *Toronto Star* newspaper's website and in its print edition. The appellant's defamation lawsuit was struck on a motion by the respondents because the appellant did not comply with the notice and limitation periods for libel in a newspaper specified in the *Libel and Slander Act* (Ontario). The appellant argued that the online version of the article was not published in a "newspaper", which is defined in the *Libel and Slander Act* as "… a paper containing public news … printed for distribution to the public and published periodically …". The Court of Appeal held that the definition of "newspaper" was not restricted to a physical newspaper. The Court of Appeal reasoned that statutory interpretation principles required that the *Libel and Slander Act* be interpreted in the context of evolving realities to apply to advances in technology that did not exist when the statute was enacted, and it would be absurd to apply different regimes for print and online versions of a newspaper. The Court of Appeal rejected the appellant's argument that a new and distinct cause of action accrues, and a new limitation period begins to run, for every day that defamatory words are published online. The court held that the statutory notice and limitation periods commenced when the plaintiff discovered the online defamation. The court dismissed the appeal. Leave to appeal has been requested ([2017] S.C.C.A. No. 377 (QL)).

2. Defamatory Blog Posts

Levant v. Awan, 2017 CanLII 35113 (SCC), involved a dispute over nine disparaging posts by the defendant lawyer, political commentator, and journalist on his Internet blog. The posts related to the plaintiff and his involvement in a dispute with *Maclean's* magazine and a related hearing before the British Columbia Human Rights Tribunal. The trial judge (2014 ONSC 6890) held that the posts were defamatory and the defence of fair comment was not available because the defendant was motivated by malice. In assessing damages, the trial judge noted that the factors usually considered when quantifying defamation damages must be examined in light of the "ubiquity, universality and utility" of the Internet, and that the Internet publication of the defamatory blog posts increased the likely readership of the posts. The trial judge awarded the plaintiff $50,000 in general damages and $30,000 in aggravated damages, and ordered the defamatory blog posts be removed from the defendant's website. The Ontario Court of Appeal (2016 ONCA 970) dismissed the defendant's appeal. The Supreme Court of Canada dismissed the defendant's application for leave to appeal.

3. Damages for Defamatory Emails

McNairn v. Murphy, 2017 ONSC 1678, involved a dispute over defamatory emails relating to a disagreement between owners of vacation condominiums in Costa Rica. The emails were sent by the defendants to recipients in four different countries, including the plaintiff and his wife in Ontario. The court held that it had jurisdiction over the defendants because there was a real and substantial connection between the defamatory emails and the province of Ontario. The court held that the emails were defamatory. The court reviewed jurisprudence on damages in Internet defamation actions, and noted that the defamatory emails "will always exist in cyberspace" and the plaintiff "cannot exercise any control over the further transmission and republication of the defamation". The court awarded general, aggravated, and punitive damages totalling $70,000 against one defendant and $90,000 against the other defendant.

F. Miscellaneous

1. Injunction Prohibiting Global Internet Search Results

Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, involved an application for an interlocutory injunction prohibiting Google Inc. and Google Canada (collectively "Google") from including the defendants' websites in search results generated by Google's worldwide search engines. The defendants used their websites to advertise and sell a product designed using the plaintiffs' trade secrets. The defendants ignored a court order prohibiting them from carrying on business through any website. Google, which was not a party to the lawsuit,

voluntarily agreed to block some but not all of the defendants' websites from Google search results. The plaintiffs applied for an interlocutory injunction against Google on the basis that Google's search sites facilitated the defendants' ongoing breach of court orders. Google argued that the court did not have jurisdiction over Google or should decline jurisdiction, and in any event should not issue the requested injunction. The chambers judge (2014 BCSC 1063) granted an injunction requiring Google to block the defendants' websites from Google's search sites worldwide. The Court of Appeal (2015 BCCA 265) dismissed Google's appeal on the basis that the injunction was within the competence of the chambers judge, did not violate any applicable legal principles or norms of freedom of speech, and was justified in the circumstances.

Google appealed to the Supreme Court of Canada. Google did not dispute that there was a serious claim or that Equustek was suffering irreparable harm. Google acknowledged that its search engine results inadvertently facilitated the harm. Nevertheless, Google argued that the injunction was not necessary to prevent the harm and was not effective in doing so, the injunction should not be granted against Google as a non-party, the injunction should not have extraterritorial reach, and the injunction violated Google's freedom of expression. In a seven-two split decision, the Supreme Court of Canada dismissed Google's appeal.

The court majority held that the injunction application invoked the classic interlocutory injunction test – is there a serious issue to be tried, will irreparable harm result if the injunction were not granted, does the balance of convenience favour granting or refusing the injunction, and ultimately would granting the injunction be just and equitable in all the circumstances. The majority held that the test had been met, and rejected all of Google's arguments. The majority noted that the jurisprudence establishes that interlocutory injunctions can be granted against non-parties and with extraterritorial effect (e.g. *Norwich* orders and *Mareva* injunctions). The majority reasoned that the problem was occurring online and globally because the "Internet has no borders", and that the only way for the interlocutory injunction be effective was to have the injunction apply globally. The court noted that Google acknowledged its ability to comply with the global injunction with relative ease. The majority held that freedom of expression issues did not tip the balance of convenience against the injunction. The majority stated that Google could apply to court to vary the injunction if there were evidence that complying with the injunction required Google to violate foreign laws, including interfering with freedom of expression. The majority reasoned: "We are dealing with the Internet after all, and the balance of convenience test has to take full account of its inevitable extraterritorial reach when injunctive relief is being sought against an entity like Google" (at para. 47). The majority concluded that the interlocutory injunction against Google should be upheld because it was the only effective way to mitigate the harm to Equustek pending resolution of the lawsuit, and any countervailing harm to Google was minimal to non-existent.

The dissenting minority would have granted the appeal and set aside the interlocutory injunction against Google on the basis that, while the chambers judge had jurisdiction to issue the injunction, the chambers judge should have exercised judicial restraint and refrained from issuing the injunction because the injunction was effectively permanent and against an innocent third party, required ongoing court supervision and modification and had not been shown to be effective, and that alternative remedies were available.

After the Supreme Court of Canada issued its decision, Google commenced proceedings against Equustek in a U.S. District Court to prevent enforcement of the Canadian injunction. Google applied for a preliminary order against enforcement of the Canadian injunction. Equustek did not oppose the application. The district court granted the preliminary order. The court reasoned that the Canadian injunction eliminated Google's immunity under United States *Communications Decency Act* (which immunizes providers of interactive computer services against liability arising from content created by third parties) and threatened free speech on the global Internet. See *Google LLC v. Equustek Solutions Inc.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

2. Liability for Fraudulent Wire Transfer Instructions

Du v. Jameson Bank, 2017 ONSC 2422, involved a dispute between the plaintiff bank customer and the defendant bank over liability for unauthorized wire transfers totalling USD $135,000 conducted by the defendant as a result of fraudulent emails sent by an unknown fraudster who allegedly hacked into the plaintiff's personal email account. The emails included details that would not ordinarily be known by a fraudster, such as the name of the plaintiff's financial advisor and his bank account at another bank. The plaintiff's account was governed by terms and conditions that the plaintiff acknowledged in writing when he opened the account. The terms and conditions permitted the plaintiff to give electronic instructions to the bank through a specified email address, and provided that the bank was entitled to rely on those email instructions and was not obligated to question them. The terms and conditions identified the risks associated with email instructions, allocated those

risks to the plaintiff and obligated the plaintiff to protect the integrity of his email account. The terms and conditions protected the bank against liability unless the bank was grossly negligent or engaged in wilful misconduct. The court held that the plaintiff was bound by the terms and conditions regardless of whether he actually read them. The court found that the bank had no reason to doubt the authenticity of the email instructions to make the fraudulent wire transfers. The court found that the bank was not negligent, and did not act improperly, by accepting the email instructions. The court held that the bank was not obligated to question the wire transfer instructions. The court reasoned that the fact that a bank customer is a victim of fraud does not result in an automatic transfer of liability to the bank. The court held that the bank was not liable for the transferred funds based on the tort of conversion, which applies to the negotiation of fraudulent cheques or other bills of exchange, because an email is not analogous to a cheque or other bill of exchange and is not a chattel that can be negotiated from party to party. The court concluded that it was the plaintiff's failure to secure his email account that led to the fraudulent wire transfers, and that the account terms and conditions were a complete defence to the plaintiff's claims against the bank. The court dismissed the action.

3. Search and Seizure of Text Messages from Recipient's Device

R. v. Marakah, 2017 SCC 59, involved an appeal from convictions for firearms offences. The convictions were based on text messages sent by Marakah to his accomplice. The police obtained the text messages as a result of an unlawful search (based on an invalid search warrant) of the accomplice's mobile phone. Marakah argued at trial that the text messages should not be admitted against him because they were obtained in violation of his *Charter* right against unreasonable search or seizure. The trial judge and a majority of the Court of Appeal held that Marakah could not have an expectation of privacy in the text messages recovered from the accomplice's mobile phone, and therefore did not have standing to challenge the admissibility of the messages. The Supreme Court of Canada, in a four-one-two split decision, allowed Marakah's appeal and set aside the convictions.

The court majority held that Marakah had standing to challenge the use of the text messages against him on the grounds that the search of the accomplice's phone violated Marakah's *Charter* rights because Marakah had an objectively reasonable expectation of privacy in the text messages. The majority reasoned that the subject matter of the search of the accomplice's phone was the electronic conversation between Marakah and the accomplice, Marakah had a direct interest in that subject matter, Marakah subjectively expected the conversation to remain private notwithstanding his lack of control over the messages, and Marakah's expectation was objectively reasonable. The majority stated that "it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging", that "people may be inclined to discuss personal matters in electronic conversations precisely because they understand that they are private", and that "privacy in electronic conversations is worthy of constitutional protection" that "should not be lightly denied". The majority also reasoned that control over messages is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest. The majority concluded that the admission of the text messages into evidence would bring the administration of justice into disrepute, and therefore the messages should have been excluded from evidence.

The dissenting minority held that a reasonable expectation of privacy requires some measure of control over the subject matter of the search. The court reasoned that "divorcing privacy from any sense of control … would distort and de-contextualize the concept of privacy, create tension with the autonomy of individuals to freely share information, depart from this Court's longstanding jurisprudence, and raise a host of practical concerns for law enforcement and the administration of criminal justice" (at para. 199). The minority concluded that Marakah could not have a reasonable expectation of privacy in the text messages because Marakah had absolutely no control over the text messages stored on his accomplice's mobile phone.

4. Search and Seizure of Text Messages from Service Provider

R. v. Jones, 2017 SCC 60, involved an appeal from convictions for firearms and drug trafficking offences. The convictions were based on text messages sent by Jones to his accomplice. The police obtained historical records of the text messages from the service provider's account for the accomplice's phone as a result of a production order issued under *Criminal Code* s. 487.012 (now s. 487.014). Jones argued at trial that the text messages should not be admitted against Jones because the production order was not the correct procedure and violated Jones' *Charter* right against unreasonable search or seizure. The trial judge held that Jones had

no standing to challenge the admissibility of the text messages, and the Court of Appeal dismissed Jones' appeal. The Supreme Court of Canada, in a five-one-one split decision, dismissed Jones' appeal.

The court majority held that Jones had a reasonable expectation of privacy in the text messages stored by the service provider, and therefore had standing to challenge the production order that resulted in disclosure of the text messages. The majority reasoned that whether a claimant has a reasonable expectation of privacy must be answered with regard to the totality of the circumstances. The majority held that the subject matter of the search was the electronic conversation between Jones and his accomplice, Jones had a direct interest in that subject matter (based on the Crown's theory that Jones authored the messages), Jones subjectively expected the conversation messages stored in the service provider's infrastructure to remain private, and Jones' expectation was objectively reasonable. The majority reasoned that it is objectively reasonable for a text message sender to expect that a service provider will maintain privacy over the messages stored in the service provider's infrastructure and not share those messages with anyone other than the intended recipient, notwithstanding the sender's lack of control over the stored messages. The majority reasoned that an expectation of privacy was consistent with contemporary social norms, a purposive approach to the *Charter*, the legislative purpose of the *Personal Information Protection and Electronic Documents Act* and approaches taken in previous decisions. The majority held that neither the absence of a contractual confidentiality agreement between Jones and the service provider, nor the fact that the production order applied to a mobile phone account used by the accomplice, deprived Jones of a reasonable expectation of privacy that was protected by the *Charter*. The majority concluded that the search and seizure of the text messages were authorized by the production order and did not violate Jones' *Charter* right. The majority dismissed the appeal.

The dissenting justice agreed that Jones had a reasonable expectation of privacy in the sent text messages, and therefore had standing under the *Charter* to challenge the production order. The dissenting justice held that the search and seizure of the text messages pursuant to the production order were invalid and breached Jones' *Charter* rights, because the police should have obtained a warrant under *Criminal Code* Part VI.

5. Sentence for Facebook Extortion

R. v. Hunt, 2017 CanLII 86655 (NL PC), involved sentencing for the offence of extortion contrary to *Criminal Code* s. 346(1). Hunt threatened to post on Facebook intimate, personal, and private photographs of his former girlfriend unless she told her friends that she and Hunt had not separated. Hunt pleaded guilty to the offence of extortion. In considering the appropriate sentence, the court noted that social media has dramatically changed the potential impact of extortion, because social media can be used to share and disseminate intimate photographs on a worldwide basis and it is impossible for the victim to limit circulation or retrieve the photographs. The court held that the sentencing principles of general deterrence and denunciation must be emphasized in imposing a sentence for extortion. The court sentenced Hunt to nine months imprisonment (less credit for pre-sentence custody), followed by two years' probation during which Hunt is prohibited from accessing the victim's Facebook page or from commenting or posting anything about her on Facebook or any other social media site.
