Canadian Internet Law Update – 2019

by Bradley J. Freedman

This paper[*] summarizes selected developments in Canadian Internet law during 2019. 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. Trademarks

1. Internet Use of Trademark

Live! Holdings, LLC v. Oyen Wiggs Green & Mutala LLP, 2019 FC 1042, involved an application to expunge the Canadian trademark registration for the trademark LIVE! on the basis that it had not been used for the services – advertising and marketing services, entertainment services and hotel services – for which it was registered. Live did not have any "bricks and mortar" facilities in Canada. The Registrar of Trade-marks decided to expunge the registration, and Live appealed. Live argued that the LIVE! trademark had been used in Canada because people in Canada were able to access websites bearing the trademark, buy tickets to entertainment events in the United States that were advertised with the trademark, and hold a reservation at a hotel in the United States bearing the trademark. The court rejected those arguments on the basis that they did not establish that any of the services for which the trademark was registered were performed in Canada. The court reasoned that the term "services", as used in the *Trade-marks Act*, is to be given a liberal but not unlimited interpretation, and that to sustain a trademark registration for services some aspect of the services must be offered to people in Canada or performed or delivered in Canada so that they receive a "meaningful and tangible benefit" in Canada without leaving Canada. The court held that the mere display of a trademark on a computer screen is not sufficient to establish use of the trademark in Canada, and that people in Canada do not receive a tangible and meaningful benefit simply by accessing a website that provides information about events or hotels in the United States or by using online reservation portals that permit them to purchase tickets or book rooms for events or hotels in the United States. The court concluded: "Although the jurisprudence suggests a trend toward an expansive view of "use" and acknowledges that we must adapt to the realities of ecommerce, the basic principle remains that the use of a trade-mark in Canada requires that the registered services or wares result in a tangible and meaningful benefit to people in Canada". The court dismissed the appeal.

2. Injunction to Continue Use of Domain Name

Canivate Growing Systems Ltd. v. Brazier, 2019 BCSC 899, involved a dispute over the ownership and use of the canivate.com domain name. The defendant, one of the plaintiff's founders, registered the domain name in his own name before the plaintiff was incorporated for use by the plaintiff in connection with its cannabis greenhouse technology business. The plaintiff used the CANIVATE trademark and the canivate.com domain name (for its website and as part of the email addresses for its employees and other personnel) in connection with its business and related start-up activities (e.g., investor-relations) for approximately one year. The defendant retained registered ownership of the domain name. After a dispute arose among the plaintiff's shareholders, the defendant disputed ownership of the canivate.com domain name and disabled the domain name so that it no longer resolved to the plaintiff's website and related email addresses no longer functioned. The defendant acknowledged that he did not intend to use the domain name, but rather disabled it to gain leverage in the shareholders' dispute. The plaintiff sued and applied for a pre-trial injunction requiring the defendant to restore the plaintiff's use of the domain name. The court held that the plaintiff had established a strong *prima facie* case of passing off and would suffer irreparable harm if an injunction were not granted, and that the balance of convenience favoured granting an injunction. The court reasoned that it would be impossible to measure the harm to the plaintiff caused by its loss of

[*] Copyright © 2020 Bradley Freedman. All rights reserved. This paper is an abridged version of a chapter in *Annual Review of Law & Practice, 2020*, Continuing Legal Education Society of British Columbia.

control over its message, disruption of its business interests while in a start-up, fundraising mode and the potential loss of confidence by investors. The court also reasoned that the defendant could easily, with a "keystroke exercise", restore the plaintiff's use of the domain name. The court granted the injunction and ordered the defendant to restore the plaintiff's use of the domain name.

B. Copyright

1. Site-blocking Order

Bell Media Inc. v. GoldTV.Biz, 2019 FC 1432, involved an application by Canadian broadcasting companies for an interlocutory mandatory injunction (a "site-blocking order") against innocent third-party Internet service providers (ISPs) requiring that they block access to websites and Internet services, operated by the anonymous defendants, that infringed copyright in the plaintiffs' programming content. The application was opposed by one of the ISPs. The court noted that a site-blocking order had not previously been issued in Canada, but had been issued in the United Kingdom. The court held that it had equitable jurisdiction to issue a site-blocking order against non-parties who had not engaged in any wrongdoing, and the provisions of the *Copyright Act* and the *Telecommunications Act* did not support the view that the court should decline to exercise its jurisdiction. The court held that an applicant for a site-blocking order was required to establish: (1) there is a serious issue to be tried; (2) irreparable harm will result if the order is not granted; (3) the balance of convenience favours issuing the order; (4) the proposed order is properly targeted; (5) the third party respondents should be justifiably bound by the order; and (6) considering the balance of convenience, the effects of the order are proportional and appropriately balance the interests of the defendants, the third party respondents, and the public. The court explained that the fundamental question is whether the granting of the site-blocking order is just and equitable in all of the circumstances, including the following principles or factors endorsed by the English Court of Appeal in *Cartier International AG v. British Sky Broadcasting Ltd.*, [2016] EWCA Civ 658: necessity, effectiveness, dissuasiveness, complexity and cost, barriers to legitimate use or trade, fairness, substitution and safeguards. The court held that the plaintiffs met the test for a site-blocking order. The court rejected the arguments that site-blocking is an extreme measure that risks inadvertently stifling free expression by blocking legitimate content, and that the impact of a site-blocking order on the ISPs and consumers outweighed any harm to the plaintiffs caused by the copyright infringing activity. The court found that a site-blocking order would be an effective means of protecting the plaintiffs' rights, even though the site-blocking process could be circumvented and the order was not directed to all Canadian ISPs. The court noted that the proposed order made provision for the technical limitations of the ISPs, recognized that the ISPs should not bear the cost of implementation, included measures to minimize the risk of over-blocking and a process to address inadvertent over-blocking, and expired after two years. The order required the plaintiffs to indemnify the ISPs for the reasonable marginal cost of complying with the order, and for reasonably incurred costs, losses and liabilities resulting from third party claims and proceedings against the ISPs as a result of their compliance with the order.

2. Application to Certify Reverse Class Action

Voltage Pictures, LLC v. Salna, 2019 FC 1412, involved an application by film production companies for certification of a "respondent class proceeding", also known as a "reverse class action", for infringement of copyright in films that were distributed using peer-to-peer networks and file sharing software. The proposed class respondents were Internet account subscribers whose accounts had been used to upload the films during the prior six-month period. The film production companies argued that the proposed class proceeding would be more efficient than the alternative of naming thousands of respondents personally in separate proceedings, particularly since statutory damages for non-commercial infringements under the *Copyright Act* are limited to $100 to $5,000. The court dismissed the certification application on various grounds. The court held that the pleadings did not allege the facts necessary to disclose a reasonable cause of action for primary or secondary copyright infringement. The court also held that the film production companies had failed to establish that there was an identifiable class of two or more respondents. The court also held that a class proceeding was not a preferable procedure because the proceeding would require multiple individual fact-findings for each class member on almost every issue, depended on the availability of uncertain public resources, would invoke the *Copyright Act* notice-and-notice regime in a way that was unsustainable and would unfairly overburden Internet service providers, did not address the possibility that members of the proposed respondent class would opt-out, and did not name a suitable representative

respondent. The court concluded that there were other available means of resolving the claims (i.e., joinder or consolidation) that were preferable to a reverse class action.

3. Application for Norwich Order

ME2 Productions, Inc. v. Doe #1, 2019 FC 214, involved an application by movie production companies for a *Norwich* order requiring a non-party Internet service provider ("ISP") to disclose the names and addresses of subscribers alleged to have illegally downloaded and shared the plaintiffs' copyright-protected movies, and for an order for damages against the ISP for failing to comply with its obligations under the notice-and-notice regime of the *Copyright Act.* The application was supported by affidavits sworn by law clerks that attached declarations by a technical consultant. The application was granted by the case management judge, and the ISP appealed. The court granted the appeal and set aside the *Norwich* order. The court held an application for a *Norwich* order should normally be served on the relevant ISP, and that the ISP could choose to participate in the application. The court emphasized that copyright owners who seek *Norwich* orders must ensure that they make full and frank disclosure of all relevant information to the court, and their motion records must be accurate, complete and organized in a manner to permit the information to be understood and verified. The court noted that it was required to consider not only the interests of copyright owners but also the privacy interests of individual subscribers whose names were subject to disclosure, and that the court was "entitled to demand the best available evidence to be filed in support of a motion seeking the extraordinary equitable relief of a *Norwich* order". The court held that the evidence filed in support of the application did not meet the standard required by the jurisprudence or the rules of court, and so the *Norwich* order could not stand. The court explained that the core evidence in support of a motion for a *Norwich* order – setting out the details of the alleged copyright infringement, the connection to a particular IP address and its association with an ISP, as well as the details regarding the notice that was sent pursuant to the notice-and-notice regime – should be contained in affidavits that can be subject to cross-examination; and if that cannot be done an affidavit explaining why, and setting out the best available evidence, should be provided. The court also held that the case management judge did not err by dealing with the claim against the ISP as part of the *Norwich* order application, rather than as a separate proceeding, because the ISP was already voluntarily participating in the application and the procedure specified by the judge would ensure that the ISP was treated fairly.

4. Application for Costs of Norwich Order

Voltage Pictures, LLC v. Salna, 2019 FC 1047, involved a proposed reverse class action against unknown defendants engaged in illegal Internet sharing of the plaintiffs' copyright-protected films. The plaintiffs brought an application for a *Norwich* order requiring a non-party Internet service provider ("ISP") to 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 action. The Supreme Court of Canada (*Rogers Communications Inc. v. Voltage Pictures, LLC*, 2018 SCC 38) previously held that the ISP was entitled to its reasonable costs of compliance with a *Norwich* order, but was not entitled to compensation for costs that the ISP should have incurred in performing its statutory obligations under the notice-and-notice regime of the *Copyright Act*. On a motion to determine the ISP's recoverable costs, the court held that the ISP was entitled to be compensated for the direct labour costs incurred to comply with the *Norwich* order, but not overhead costs, employee benefits or administrative time. The court reasoned that reasonable compensation to an ISP for compliance with a *Norwich* order must be "directly tied" to complying with the order.

5. Obituary Piracy

Thomson v. Afterlife Network Inc., 2019 FC 545, involved a class proceeding against the defendant for operating a website (www.afterlife.co/ca) that reproduced over one million obituaries and accompanying photos taken from websites of Canadian funeral homes and newspapers, and displayed revenue-generating advertising for third party businesses and sales of flowers and virtual candles. The website terms of use asserted that the defendant owned copyright in the website contents. The class members, relatives of the deceased who wrote the copied obituaries, complained that the defendant's unauthorized use of the obituaries for commercial purposes caused people to believe they had consented to, and were profiting from, the commercial use of the obituaries. The defendant removed some obituaries at the request of some relatives, but refused other requests. The defendant shut down the website approximately one month after the proceeding was commenced, and directed Internet traffic to a similar website (Everhere) that used

obituaries in template form rather than exact copies from other websites. The defendant did not respond to the class proceeding. The court found that the copied obituaries and photographs were original works protected by copyright, and held that the defendant infringed the class members' copyright in the obituaries and photographs. The court held that the class members had failed to provide the objective evidence required to support a finding that their moral rights in the copied obituaries had been infringed. The court found that the defendant's "obituary piracy" was high-handed, callous and reprehensible, and caused the class members to suffer significant emotional harm. The court issued a wide injunction against the defendant and its director (who was also a director of the company operating the Everhere website) prohibiting future infringements. The court awarded the class members $10 million statutory damages and $10 million aggravated damages.

6. Copyright Infringement by Music Video Streaming

Young v. Thakur, 2019 FC 835, involved a dispute over the respondents' unauthorized online streaming of a music video featuring a song written and recorded by one of the applicants. The applicants engaged the respondents to create a music video that featured the song. There was no written contract, and no discussion about copyright ownership or permission to use the song, sound recording or music video. A dispute arose between the parties, and the respondents refused to give the music video to the applicants. Instead, the respondents made the music video (including the sound recording) available for streaming on their website and Vimeo. The respondents refused to comply with the applicants' demand to stop streaming the music video until after the applicants commence legal proceedings. The court held that the respondents' streaming of the music video constituted an unauthorized reproduction, and copyright infringement, of the song (a musical work) and the sound recording of the applicant's performance of the song. The court reasoned that the applicants authorized the respondents to use the song and sound recording for the sole purpose of creating the music video, and did not give the respondents permission to use (stream) the music video and thereby reproduce the song or sound recording. The court held that the applicants had failed to provide the evidence required to support a finding of infringement of their moral rights in the song and sound recording. The court held that an injunction was warranted to ensure that the respondents did not repost the music video. The court awarded the applicants statutory damages of $2,000 ($1,000 for each work – the song and sound recording – infringed). The court refused to order the respondents to deliver up the raw video footage, because the applicants did not establish any rights to the raw video footage.

C. Electronic Contracts and Electronic Transactions

1. Arbitration Clause Held Unenforceable

Heller v. Uber Technologies Inc., 2019 ONCA 1, involved a proposed class action on behalf of Uber drivers seeking a declaration that the drivers are governed by the Ontario *Employment Standards Act* and damages of $400 million against Uber for violating the Act. Uber applied for an order staying the action on the basis of an arbitration clause in the Uber services agreement that all drivers must accept by twice clicking "Yes, I Agree" the first time they log into the Uber App. The clause required mandatory mediation and then arbitration in Amsterdam, and required a complaining driver to pay an up-front administrative/filing fee of US$14,500. The motions judge granted the stay, and the plaintiff appealed. The court of appeal held that the motions judge made palpable and overriding errors. The court held that the arbitration clause was invalid because, based on the presumption that drivers are employees of Uber (as pleaded), the clause constituted a prohibited contracting out of the provisions of the *Employment Standards Act*. The court also held, as a separate and independent conclusion, that the arbitration clause was invalid on the basis of unconscionability at common law. The court reasoned that: (1) the arbitration clause represented a "substantially improvident or unfair bargain" because it required an individual driver with a small claim to incur the significant costs of arbitrating the claim in Amsterdam (Uber's home jurisdiction) under the laws of the Netherlands, after paying a US$14,500 administrative fee that was out of all proportion to the amount that may be involved; (2) drivers did not have any legal or other advice before entering into the services agreement, and were not able to negotiate any of the terms of the services agreement; (3) there was a significant inequality of bargaining power between drivers and Uber; and (4) Uber knowingly and intentionally chose the arbitration clause to favour itself and take advantage of drivers, who were clearly vulnerable to Uber's market strength. The court emphasized that the arbitration clause "was much more than just a simple arbitration provision" found in normal commercial contracts, and operated to defeat the very claims it purported to resolve. The court also reasoned that the drivers were "very much akin to

consumers in terms of their relative bargaining position", were at the mercy of the terms, conditions and rates of service set by Uber, and had only one choice – click "I agree" with the terms of the contractual relationship presented by Uber – if they wished to be an Uber driver. For those reasons, the court held the arbitration clause to be invalid and set aside the stay of the class action. The Supreme Court of Canada granted Uber's application for leave to appeal, and the appeal was heard and reserved on November 6, 2019. (*Uber Technologies Inc. v. Heller*, [2019] S.C.C.A. No. 58 (QL)).

2. Electronic Contract for Condo Sale

1353141 Alberta Ltd v. Roswell Group Inc., 2019 ABQB 559, involved a dispute between family members over an alleged agreement for the purchase of an interest in a business condominium. The agreement was formed by way of an exchange of emails between the parties' respective solicitors. The defendant's solicitors sent an email setting out a "multi-faceted offer" in the form of a shotgun structure with four options. The plaintiff's solicitors sent a reply email that accepted one of the proposed options. The defendant refused to complete the transaction. The court held that an email from the defendant's solicitors was an offer that was capable of acceptance, and that the solicitors had legal authority to make the offer on behalf of the defendant. The court further held that the emails contained the three essential terms of a binding contract – parties, property and price. The court further held that an interest in land can be transferred without a formal contract, as long as there is compliance with the *Statute of Frauds*. The court held that the emails satisfied the *Statute of Frauds* requirement that an agreement for the sale of land be in writing and signed by the party to be charged therewith. The court reasoned that the "block electronic signature" at the end of the defendant's solicitor's offer email satisfied the signature requirement because the source and authenticity of the email were clear and the block signature established the solicitor's approval of the email's contents. The court noted that the Alberta *Electronic Transactions Act* does not apply to records that create or transfer interests in land, but reasoned that the court could still rely on the broad definition of "writing" in the Alberta *Interpretation Act* to find that the emails satisfied the *Statute of Frauds* writing requirement.

3. Settlement Agreement Made by Email

Lumsden v. Toronto (City) Police Services Board, 2019 ONSC 5052, involved an application to enforce a settlement agreement made by an exchange of emails. The emails set out the details of the settlement, including a requirement that the plaintiffs execute a "full and final release". A few days later, the plaintiffs took the position that the emails did not result in a binding settlement because the parties had not agreed to the terms of the release. The court held that a binding settlement can be formed by emails (i.e., formal minutes of settlement are not required), and a full and final release is an implied term of a settlement that has already been reached. The court explained that a settlement is not tentative, or an "agreement to agree", merely because the parties must still agree on the wording of a release. The court held that it was not open to the plaintiffs to object to the release proposed by the defendants, and they could not rely on it to resile from the settlement agreement. The court ordered the action be dismissed on the terms of the settlement agreement, and ordered that the plaintiffs be deemed to have executed the release proposed by the defendants.

4. Jurisdiction Over Email Contract Dispute

Real Crowd Capital Inc. v. 1034179 B.C. Ltd., 2019 ONSC 2908, involved a dispute over commissions alleged to be payable with respect to the financing of a real estate project in British Columbia. The defendant British Columbia real estate company engaged the plaintiff Ontario company as its agent to secure financing for the project. The arrangement was set out in a letter agreement that the plaintiff delivered to the defendant's directors located in British Columbia. The directors accepted the offer, signed the letter in British Columbia and returned it by email to the plaintiff in Ontario. The relationship then broke down, and the plaintiff commenced a lawsuit in Ontario for payment of commissions. The defendant brought an application to stay the lawsuit on the basis that the court lacked jurisdiction and alternatively that British Columbia was a more convenient forum. The court dismissed the application. The court applied the conventional rule that contracts are formed in the place where acceptance is received, and held that the letter agreement was a contract formed in Ontario. The court reasoned that the language of the letter agreement, which stated that the agency arrangement was established by acceptance of the letter, did not displace the general contract formation rule that a contract is not formed until acceptance of an offer is communicated. The court further held that the defendant failed to show that British Columbia was clearly the more appropriate forum.

5. Electronic Union Membership Cards

United Steelworkers Union v. Toronto and York Region Labour Council, 2019 CanLII 123094 (ON LRB), involved an unopposed application to the labour relations board to accept electronic evidence of union membership in support of a certification application. The union membership cards were created using a process that involved electronically signed (using a "draw" function) applications, identity verifying emails and an audit trail, and resulted in an encrypted electronic union membership card. The board decided to accept the electronic evidence on the basis that the security features used to protect the electronic union membership evidence were arguably stronger protections than the traditional paper membership card.

6. IIROC Confirms Use of Electronic Signatures

In March 2019, the Investment Industry Regulatory Organization of Canada ("IIROC") issued Guidance Note 19-0051 to confirm that electronic signatures may be used to satisfy signature requirements under various IIROC rules. The Note explains that regulated firms should have appropriate policies and procedures in place for compliance with signature requirements, and should act in good faith in applying those policies and procedures. The Note reminds firms to consider other applicable laws relating to signatures on documents.

7. Electronic Chattel Paper

In May 2019, the Ontario *Personal Property Security Act* and the Saskatchewan *Personal Property Security Act* were amended to permit the use of electronic chattel paper. The amendments bifurcate the definition of "chattel paper" into "tangible chattel paper" (i.e., chattel paper evidenced by a record or records consisting of information inscribed on a tangible medium) and "electronic chattel paper" (i.e., chattel paper created, recorded, transmitted or stored in digital form or other intangible form by electronic, magnetic or optical means). The amendments also add provisions that specify how electronic chattel paper may be perfected through "control". The amendments have been given royal assent, but have not been proclaimed in force.

D. Internet Defamation

1. Defamatory Postings on Doctor Rating Websites

Zoutman v. Graham, 2019 ONSC 2834 and 2019 ONSC 4921, involved a dispute over defamatory comments about the plaintiff physician posted by the defendant to the RateMDs.com and OntarioDoctorDirectory.ca websites. The defendant had never been a patient of the plaintiff, who had testified as an expert witness in a clinical negligence trial involving the death of the defendant's brother. Commencing the day after the plaintiff testified at the trial, the defendant commenced a campaign, lasting for approximately one and a half years, during which the defendant posted defamatory comments about the plaintiff to the websites. The court rejected the defendants anti-SLAPP motion to dismiss the lawsuit on various grounds, including the fact that the public interest in permitting the lawsuit to continue outweighed any public interest in protecting the defendant's expression. The court rejected the defendant's denial of responsibility for most of the defamatory postings. The plaintiff did not provide any direct evidence that any individual had read the defamatory postings. Nevertheless, the court inferred from the totality of the circumstances – including the prominence of the RateMDs.com and OntarioDoctorDirectory.ca profile in Google searches concerning the plaintiff – that the postings had been read and therefore had been published. The court rejected the defendant's defence of fair comment, and found that the defendant acted out of malice. The court awarded the plaintiff $25,000 general damages, $25,000 aggravated damages, and $50,000 costs. The court also issued a permanent injunction against the defendant preventing him from writing, speaking, publishing, posting or otherwise disseminating any defamatory content on the Internet or any other medium, electronic or otherwise, directly or indirectly relating to the plaintiff.

2. Defamatory Postings on Social Media

Emeny v. Tomaszewski, 2019 ONSC 3298, involved a dispute over defamatory statements about the plaintiff posted by the defendant to social media sites. The statements falsely asserted that the plaintiff was a sexual predator who commits illegal acts and drugs women without their consent. The defendant did not respond to, or make any attempt to defend, the lawsuit. The plaintiff claimed that the use of social media to

publish the defamatory statements was especially damaging because they caused the "near total destruction" of the plaintiff's career and caused the plaintiff to suffer serious mental health problems. The court found that the statements were defamatory and reflected a sustained attempt to damage the plaintiff's personal and professional reputation, and that the use of social media amplified the impact of the defamatory statements. The court awarded the plaintiff $250,000 general damages, $100,000 special damages for lost income and $100,000 punitive damages. The court also granted a permanent injunction enjoining the defendant from publishing statements or comments about the plaintiff, because it was not possible to determine whether the defendant intended to publish defamatory statements in the future and it appeared likely that the plaintiff would be unable to enforce the damages judgment against the defendant.

3. Defamatory Postings on Instagram

Rook v. Halcrow, 2019 BCSC 2253, involved a dispute over defamatory postings on Instagram and other websites. The plaintiff alleged that the defendant made the postings after the plaintiff ended their romantic relationship. The postings, which were widely read, falsely claimed that the plaintiff was a heartless cheater, an alcoholic and drunkard and had sexually transmitted diseases. The defendant denied making the postings, but did not take the stand herself or call any evidence. The court found that the postings were made by the defendant out of spite and animosity, and for the purpose of injuring the plaintiff. The court found that the defendant was motivated by malice to mount a relentless and extensive defamation campaign against the plaintiff. The court awarded the plaintiff $175,000 general damages, $25,000 aggravated damages, special damages to compensate for amounts paid by the plaintiff for the services of reputation consultants to assist in having the postings removed, and costs. The court also issued a permanent injunction restraining the defendant from publishing any of the defamatory statements.

4. Defamatory Emails

Malak v. Hanna, 2019 BCCA 106, involved a dispute over defamatory postings on various websites and YouTube and in emails, all designed to harm the plaintiffs to gain a competitive advantage in the traffic flagging services business. The trial judge found the defendants liable, and the defendants appealed on various grounds. Some of the impugned emails did not contain any defamatory statements, rather they contained only a hyperlink to websites containing defamatory statements. On appeal, the court of appeal held that the trial judge erred in finding those emails to constitute defamatory statements. The court followed the Supreme Court of Canada decision in *Crookes v. Newton*, 2011 SCC 47, and held: (1) "the use of a hyperlink to defamatory content does not, by itself, amount to publication even if the hyperlink is followed and the content accessed"; (2) "when a person follows a hyperlink to defamatory content it is the actual creator or poster of that content who has published the libel"; and (3) "only when a hyperlinker presents content from the hyperlinked material in a way that actually repeats the defamatory content, should that content be considered to be 'published' by the hyperlinker". The court allowed the appeals in part, and ordered a new trial on certain liability issues.

5. Limitation Period for Online Defamation

AARC Society v. Canadian Broadcasting Corporation, 2019 ABCA 125, involved a dispute over alleged defamatory statements in a CBC television program that was posted on the CBC website, then removed from the website, and then reposted on the website. The plaintiff applied to amend its claim and the chambers judge refused the application on various grounds. On appeal, a majority of the court of appeal allowed the appeal but disagreed as to whether a defamatory website posting is governed by the "single-publication rule" (as adopted by the Ontario Court of Appeal in *John v. Ballingall*, 2017 ONCA 579) or the "multiple-publication rule" (as adopted by the British Columbia Court of Appeal in *Carter v. B.C. Federation of Foster Parents Assn.,* 2005 BCCA 398). The Supreme Court of Canada refused CBC's application for leave to appeal (2019 CanLII 99449). See also *Torgerson v. Nijem*, 2019 ONSC 3320.

6. Defamatory Hate Speech

Paramount v. Kevin J. Johnston, 2019 ONSC 2910, involved a dispute over the defendants' false and malicious Islamophobic hate speech directed against the plaintiff restaurant chain and its owner and published on the defendants' website, YouTube channels, Twitter accounts, Facebook accounts and other social media accounts and websites. The defendants responded to the plaintiffs' lawsuit by continuing their defamatory and harassing campaign against the plaintiffs, evading service, harassing the plaintiffs' counsel,

breaching numerous court orders, and repeatedly disrespecting the court process and publishing statements expressing contempt for the proceeding and maligning the court and its judges. The court found the defendants' statements to be defamatory of the plaintiffs, and held there were no available defences. The court noted that defamatory statements disseminated over the Internet must be examined in light of the "ubiquity, universality and utility" of the Internet, and observed that "the truth rarely catches up with a lie". The court found that the defamatory statements were deeply damaging to the plaintiffs from both a business and personal perspective, caused irreparable reputational harm and caused the plaintiffs' to lose a lucrative business opportunity. The court found the defendants would likely continue to publish defamatory statements about the plaintiffs, and there was a real possibility that the defendants would refuse or be unable to pay any judgment. The court awarded the plaintiffs general, aggravated, punitive, and special damages in the amount of $2.5 million, and granted a permanent injunction restraining the defendants from making any defamatory statements about the plaintiffs.

E. Canada's Anti-Spam Legislation ("CASL")

In 2019, the Canadian Radio-television and Telecommunications Commission ("CRTC") continued to enforce Canada's Anti-Spam Legislation (commonly known as "CASL") and issue guidance for CASL compliance.

1. Enforcement

In April 2019, the CRTC issued a decision imposing a $100,000 administrative monetary penalty against the President/CEO of a corporation known as "nCrowd" for CASL violations (i.e., sending promotional emails without the recipients' consent and without a properly functioning unsubscribe mechanism) committed by nCrowd and its subsidiaries. The CEO was held personally liable because he "acquiesced", which the CRTC interpreted to mean "agreeing to something tacitly, silently, passively, or without protest", in nCrowd's CASL violations. No order was made against nCrowd because it had been dissolved.

In December 2019, the CRTC issued a notice of violation imposing administrative monetary penalties totaling $115,000 against two individuals operating a partnership known as "Orcus Technologies" for allegedly developing, selling, and promoting malware known as "Orcus RAT", which enables hackers to install the program and take control of a victim's computer without their knowledge or consent. In addition, one of the individuals operated a dynamic domain name server service used by hackers to install malware on computer systems and to communicate with the infected computer systems in Canada and abroad.

2. Guidance

In August 2019, the CRTC issued *Enforcement Advisory - Notice for businesses collecting customer data with in-store WiFi* to explain the "Social WiFi" business model, and remind businesses and consumers of CASL requirements for sending marketing messages to individuals who subscribe to Social WiFi.

In October 2019, the CRTC issued *Enforcement Advisory - Notice for Web Hosting Service Industry* to remind web hosting providers and operators of other networked infrastructure that they must not contravene CASL by aiding, inducing, procuring, or causing to be procured the distribution of malware, and to encourage those organizations to exercise due diligence and establish a CASL compliance program.

F. Cybercrime and Cybersecurity

1. Liability for Cybercrime Loss

St. Lawrence Testing & Inspection Co. Ltd. v. Lanark Leeds Distribution Ltd., 2019 CanLII 69697 (ON SCSM), involved a dispute over a misdirected $7,000 settlement payment made based on fraudulent email instructions. The settlement agreement required the defendant to pay the settlement amount to the plaintiff's lawyers' trust account at a specified bank. Before the defendant paid the settlement payment, a cybercriminal hacked the email account of a paralegal employed by the plaintiff's lawyers, and sent the defendant fraudulent emails with instructions to make the payment to a different bank account in the name of an individual (rather than the plaintiff's lawyers). The defendant paid the settlement amount to the criminal's account in accordance with the fraudulent instructions. The funds were not recovered. The plaintiff applied to court for an order that the defendant pay the settlement amount to the plaintiff, and the

defendant argued that it had already made the required payment in accordance with email instructions sent from the paralegal's email account. The defendant relied on the decision in *Du v. Jameson Bank* and argued that the plaintiff should bear the loss resulting from the cybercrime. The court distinguished *Du v. Jameson Bank* on the basis that in that case the governing account agreement allocated the risk of email fraud. The court held that where a cybercriminal takes control of the email account of "Victim A" and, impersonating Victim A, sends instructions to "Victim B" to transfer funds intended for Victim A (or a third party) to the criminal's account, Victim A is not liable for the loss unless: (1) Victim A and Victim B are parties to a contract that authorizes Victim B to rely on email instructions from Victim A and, assuming compliance with the contract, shifts liability for loss resulting from fraudulent payment instructions to Victim A (as in *Du v. Jameson Bank*); (2) there is evidence of willful misconduct or dishonesty by Victim A; or (3) there is negligence on the part of Victim A. The court reasoned that where a home or business computer is hacked and used to send fraudulent emails to the computer owner's email contacts requesting payments to the hacker's account, the computer owner would not be liable to reimburse the fraud victims if the computer owner took reasonable and recommended security precautions for its email account. The court held that there was no evidence that the hacking of the paralegal's email account was the result of any negligence on the part of the plaintiff's lawyers or the paralegal. The court concluded that the defendant had to bear the loss resulting from the fraudulent emails, and the plaintiff was entitled to a judgment requiring the defendant to pay the settlement amount to the plaintiff. The court commented that computer fraud is an area that would benefit from legislation to establish clear principles and guidelines for the allocation of liability in the event of computer fraud. See also *Opus Consulting Group Ltd. v. Ardenton Capital Corp.*, 2019 BCSC 1847.

2. OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting

In January 2019, the Office of the Superintendent of Financial Institutions ("OSFI") issued an Advisory setting out OSFI's expectations for federally regulated financial institutions ("FRFIs") regarding the prompt reporting of "high or critical severity" technology and cyber security incidents. The Advisory defines "technology or cyber security incident" as an incident that has "the potential to, or has been assessed to, materially impact the normal operations of a FRFI, including confidentiality, integrity or availability of its systems and information". The Advisory explains that "materiality" should be defined by the FRFI in its incident management framework. The reporting requirements apply to incidents assessed by a FRFI to be of a "high or critical severity level". FRFIs must submit an initial report as promptly as possible, but no later than 72 hours after determining that a technology or cyber security incident meets the incident characteristics in the Advisory. FRFIs must submit subsequent updates on a regular basis as new information becomes available and until all relevant details about the incident and its remediation have been provided to OSFI. In addition, after incident containment, recovery and closure, OSFI expects FRFIs to report on their post-incident review and lessons learned.

3. IIROC Imposes Mandatory Reporting of Cybersecurity Incidents for Regulated Investment Firms

In November 2019, the Investment Industry Regulatory Organization of Canada ("IIROC") amended its rules to require mandatory reporting of cybersecurity incidents by IIROC-regulated investment firms. The amended rules require firms to provide IIROC with an initial report within three days of discovering a reportable "cybersecurity incident", and a comprehensive investigation report within 30 days of discovering the incident. The rules define "cybersecurity incident" as including any act to gain unauthorized access to, disrupt or misuse a firm's information system, or information stored on an information system, that has resulted in, or has a reasonable likelihood of resulting in, any of the following outcomes: (1) substantial harm to any person (which includes a natural person or legal entity); (2) a material impact on any part of the firm's normal operations; (3) invoking the firm's business continuity plan or disaster recovery plan; or (4) the firm being required by any applicable law to provide notice to any government body, securities regulatory authority or other self-regulatory organization. A firm's failure to comply with the cybersecurity incident reporting obligations could result in IIROC imposing potentially significant financial penalties or other sanctions on the firm. IIROC's *Frequently Asked Questions – Mandatory Cybersecurity Incident Response* provides important guidance for compliance with the amended rules.

G. Criminal Law

1. Constitutionality of Child Luring Investigation Technique

R. v. Mills, 2019 SCC 22, involved an appeal from a conviction for Internet child luring under *Criminal Code* s. 172.1. A police officer posed online as a 14-year-old girl with the intent of catching Internet child lurers. The officer used Facebook and email to communicate with Mills. Without obtaining prior judicial authorization under Criminal Code s. 184.2, the officer used screen capture software to create a record of his online communications with Mills as evidence for trial. The trial judge held that the police violated Mills' rights under *Charter* s. 8 because Mills had a reasonable expectation of privacy in the messages, and the screen capture software generated a seizure of the communications without prior judicial authorization. The court of appeal held that the trial judge erred in concluding that Mills had a reasonable expectation of privacy in the communications and that prior judicial authorization was required. Mills appealed.

In a three-two-one-one split decision, a majority of the Supreme Court of Canada held that Mills did not have an objectively reasonable expectation of privacy in his electronic communications with the police officer posing as a child, and consequently judicial authorization to record the communications was not required. Abella, Gascon, and Brown JJ. held that Mills could not claim an objectively reasonable expectation of privacy because he was communicating with someone he believed to be a child who was a stranger to him. The justices held that, based on the normative standard of privacy expectations described by the court in previous decisions, adults cannot reasonably expect privacy online with children they do not know. The justices reasoned that the investigative technique did not significantly reduce the sphere of privacy enjoyed by Canadians because the technique permitted the state to know from the outset that the accused would be communicating with a fictitious child he did not know. The justices noted that the Internet allows for greater opportunities to sexually exploit children, and that enhancing protection to children from becoming victims of sexual offences is vital in a free and democratic society. Wagner C.J. and Karakatsanis J. held that there was no search and seizure within the meaning of *Charter* s. 8 because the police did not interfere with a private conversation between other individuals; rather they directly participated in the conversation. The justices reasoned that an individual cannot reasonably expect their communications to be kept private from the intended recipient of the communications (even if the intended recipient is an undercover police officer). Moldaver J. agreed with the reasons of the majority. Martin J. dissented, and held that the police violated *Charter* s. 8.

2. Child Luring Provisions – Unconstitutional Presumption of Belief

R. v. Morrison, 2019 SCC 15, involved an appeal from a conviction for Internet child luring under *Criminal Code* s. 172.1(1)(b). The Supreme Court of Canada held that *Criminal Code* s. 172.1(3), which provides that if the person with whom an accused was communicating was represented to the accused as being underage then the accused is presumed to have believed that representation absent evidence to the contrary, violated the right to be presumed innocent under *Charter* s. 11(d) and was not justified under *Charter* s. 1.

3. Voyeurism Conviction for Unauthorized Screenshots

R. v. Trinchi, 2019 ONCA 356, involved an appeal from a conviction for voyeurism under *Criminal Code* s. 162(1). The appellant and the complainant were in a long-distance romantic relationship, and engaged in intimate webcam video chats. Both were naked and knew they were on a live video stream. Without the complainant's knowledge, the appellant created screenshots of the complainant and preserved the images as still photos. After the relationship ended, the appellant emailed the photos to many people. The appellant was charged with voyeurism and distribution of nude photos. The appellant was convicted of the voyeurism offence, but not the distribution offence. The appellant appealed. The court of appeal held that the complainant had a reasonable expectation of privacy, within the meaning of *Criminal Code* s. 162(1), during the video chats because, while she willingly and knowingly appeared on camera for the purpose of displaying herself naked and in sexual poses, she "did not know and did not expect that the appellant would make any permanent recording of her naked body". The court reasoned that its conclusion was "consistent with Parliament's object in enacting the voyeurism offence to protect individuals' privacy and sexual integrity, particularly from new threats posed by the abuse of evolving technologies". The court further held that the appellant acted "surreptitiously", within the meaning of *Criminal Code* s. 162(1), because he created

screenshots with the intention that the complainant be unaware he was doing so. The court dismissed the appeal. See also *R. v. Jarvis*, 2019 SCC 10.

4. Court Refuses to Order Disclosure of Smartphone Password

R. v. Shergill, 2019 ONCJ 54, involved an application for an assistance order under *Criminal Code* s. 487.02 to compel the accused to disclose the password to his locked smartphone so the police could search it pursuant to a search warrant. The court refused to issue the order on the basis that compelling the accused to "reveal the password currently buried only in his mind" would violate the accused's right under *Charter* s. 7 to not be deprived of liberty except in accordance with the principles of fundamental justice, including protection against self-incrimination and the related right to remain silent. The court distinguished other circumstances in which an accused can be required to provide or create evidence (e.g., DNA samples, fingerprinting, breathalyzer) because the assistance order sought would require the accused to "speak his mind" to the police. The court reasoned, "To construe the unlocking of the device as anything other than a manifestation of compelled speech is not, in my view, a realistic way of looking at what would be required …". The court acknowledged that digital technologies present challenges to effective law enforcement and the protection of privacy, and that a different approach to the issue of locked devices might be warranted through legislative initiatives or new jurisprudence by appellate courts. The court concluded, based on controlling authority, that the requested assistance order could not be granted.

5. Incarceration for Distributing Intimate Images

R. v. Borden, [2019] N.J. No. 118 (QL) (NLPC), involved a sentencing for the offence of distributing intimate images without consent contrary to *Criminal Code* s. 162.1(1). After the accused's relationship with her partner ended, her partner started a new relationship with another woman, Ms. X. The accused obtained nude and intimate photographs of Ms. X, and posted the photographs on Facebook and the Plenty of Fish online dating platform. Ms. X was humiliated and embarrassed. The accused pleaded guilty to the offence of distributing intimate images without consent. The court refused to grant a discharge or impose a conditional sentence on the basis that the offence was too serious and required a sentence that reflected the principles of deterrence and denunciation. The court noted that the offence of distributing intimate images is a sexual offence that is "designed to protect the personal autonomy and sexual integrity of the individual". The court imposed a sentence of 90 days' incarceration, to be served on an intermittent basis, and two years of probation.

H. Internet Business Practices and Advertising/Marketing

1. CRTC Internet Code for Internet Service Providers

In July 2019, the Canadian Radio-television and Telecommunications Commission (CRTC) issued *Telecom Regulatory Policy CRTC 2019-269* to establish the *Internet Code* (the "Code"), a mandatory code of conduct for specified, large facilities-based Internet service providers ("ISPs") that provide retail fixed Internet access services to individual customers. The stated objectives of the Code are to make it easier for Canadians to understand their Internet service contracts, to prevent bill shock from overage fees and price increases, and to make it easier for Canadians to switch ISPs. The Code takes effect on 31 January 2020, and applies in full to all renewed, amended, or extended contracts. Certain provisions of the Code also apply to existing contracts. The Code imposes detailed restrictions and requirements on ISPs (e.g., clarity in offers, contracts and related documents, including a critical information summary, provision of contracts, restrictions on changes to contracts, data usage notifications, limits on early cancellation fees, and restrictions on disconnection and information retention) and provides rights to customers (e.g., trial periods and contract cancellation). Customers who believe their ISP is not adhering to the Code must first try to resolve the problem directly with the ISP, and if they are not satisfied with the ISP's response they can file a complaint with the CRTC.

2. Online Misleading Advertising – Drip Pricing

In June 2019, the Competition Bureau announced the settlement of its enforcement action against Ticketmaster LLC and related companies ("Ticketmaster") for alleged misleading pricing advertising on a number of its websites (e.g., ticketmaster.ca, ticketsnow.com and ticketweb.ca) and on mobile applications. The Bureau's investigation concluded that Ticketmaster's advertised prices were not attainable because

they added mandatory fees (more than 20% and, in some cases, over 65%) to the advertised prices during the later stages of the purchasing process. This practice, known as "drip pricing", resulted in consumers paying higher prices than advertised. In the Bureau's view, the price representations were misleading even though the amount of the fees was disclosed before consumers completed their transaction. As part of the settlement, Ticketmaster agreed to pay a $4 million penalty and $500,000 for the Bureau's investigation costs, and to establish an advertising law compliance program.

3. Online Marketing

In October 2019, the Competition Bureau announced that it had entered into a temporary consent agreement with FlightHub Group Inc. that prohibits FlightHub from using false or misleading marketing practices on flighthub.com and justfly.com. The consent agreement is in place while the Bureau continues its investigation into FlightHub's marketing practices. The Bureau is investigating FlightHub's representations for flight-related services (e.g., seat selection and flight cancellation) and related fees, and allegations that the price of flights sometimes increases after consumers have selected their flights. FlightHub is cooperating with the Bureau's investigation.

I. Miscellaneous

1. Electronic Evidence – *Canada Evidence Act*

R. v. Ball, 2019 BCCA 32, involved an appeal from a conviction for arson and breaking and entering. One of the grounds of appeal was that the trial judge erred by admitting into evidence photographs of Facebook messages without complying with the electronic evidence provisions in the *Canada Evidence Act*. The court of appeal commented on the electronic evidence provisions as follows: (1) the provisions do not affect any rule of evidence except rules relating to authentication and best evidence; (2) the provisions do not determine the ultimate admissibility of electronic evidence, which also depends on the purpose for which the evidence is tendered and related general rules of evidence (e.g., rules regarding relevance, hearsay, character and opinion evidence); (3) the statutory rule relating to authentication codifies the common law – the burden of proof is on the tendering party and the threshold is low; (4) whether authenticated evidence is genuine is a question of weight for the fact-finder; (5) the statutory best evidence rule is intended to help ensure that an electronic document accurately reflects the original information input into a computing device by its author; (6) the standard of proof for the statutory best evidence rule is the balance of probabilities; and (7) courts adopt a "functional approach" to the interpretation and application of the electronic evidence provisions. The court noted that the photographed Facebook messages were extremely important Crown evidence and the accused contended they were tampered with, but the trial judge did not properly consider the admissibility of the evidence within the framework of the electronic evidence provisions. The court held that the trial judge committed a procedural error by failing to carefully scrutinize the admissibility of the Facebook messages evidence, which compromised the trial fairness and contributed to a miscarriage of justice. The court concluded that the cumulative effect of the errors and irregularities in the trial rendered it unfair and resulted in a miscarriage of justice. The court allowed the appeal, set aside the conviction and ordered a new trial. See also *R. v. C.B.*, 2019 ONCA 380; *R. v. S.H.*, 2019 ONCA 669; and *R. v. Durocher*, 2019 SKCA 97.

2. Cyber Bullying

Candelora v. Feser, 2019 NSSC 370, involved the first action for cyberbullying under the *Intimate Images and Cyber-Protection Act* (Nova Scotia). The cyberbullying occurred in connection with a family law dispute, and involved repeated offensive, publicly accessible Facebook postings intended to embarrass, intimidate, harass and humiliate the applicant and pressure her to abandon her claims in the family law dispute. The respondents raised various defences, which the court held were generally baseless. The court concluded that the respondents had engaged in cyberbullying. The court ordered the respondents to stop making any further cyberbullying communications about the applicant, take down and disable access to all cyberbullying communications (including Facebook postings) about the applicant, and not communicate directly or indirectly with the applicant. The court invited further submissions on the issues of damages and costs.

3. Jurisdiction Over Wrongful Death Lawsuit

Vahle v. Global Work & Travel Co. Inc., 2019 ONSC 3624, involved claims against the defendant travel agency that offered a "Teach in Thailand" experience accepted by two sisters from Ontario. The defendant was based in Vancouver, and marketed itself using social media to clients across Canada. The sisters booked the travel experience by completing the defendant's online forms, and the applicable terms and conditions provided that the agreement was governed by the laws of Canada. On a day off from their work in Thailand, while riding a motor scooter together, the sisters were struck by a car. One sister died and the other was seriously injured. The surviving sister and her parents commenced a lawsuit in Ontario against the defendant for breach of contract, breach of trust, negligence, misrepresentation and other torts. The defendant brought an application to dismiss or stay the lawsuit on the basis that the Ontario court lacked jurisdiction, and that Ontario was not the convenient forum for the dispute. The court dismissed the motion. The court considered the following circumstances regarding *jurisdiction simpliciter*: (1) the sisters' contracts with the defendant were made in British Columbia, because the sisters' completed online forms were received by the defendant in British Columbia; (2) the defendant's alleged misrepresentations were made in Ontario, because the representations were received and relied on by the sisters in Ontario; and (3) the defendant had no physical presence in Ontario, but carried on business in Ontario because it engaged in electronic commerce in Ontario by contacting (by email and telephone) and contracting with travelers in Ontario. The court held that the defendant had not rebutted the presumptive connecting factors that established a real and substantial connection between Ontario and the subject matter of the lawsuit. The court further held that the defendant had not established that Thailand, or any other jurisdiction, was a clearly more convenient or appropriate jurisdiction for the lawsuit, particularly given the broader issues of fairness to the parties and efficiency.

4. Employment Law – Prohibited Computer Use Not Cause for Dismissal

Menard v. Centre for International Governance Innovation, 2019 ONSC 858, involved a claim for wrongful dismissal. The plaintiff had been employed by the defendant as its Vice-President Finance. The defendant terminated the plaintiff's employment without cause or notice. The plaintiff sued for wrongful dismissal, and the defendant raised a defence of "after-acquired" cause – the plaintiff's unauthorized use of peer-to-peer software to illegally download copyright-protected movies, television shows and music to his work computer in violation of the defendant's internal policies (which the plaintiff had approved as a member of the defendant's senior management team). The court held that the plaintiff's use of peer-to-peer software and illegal downloading of entertainment materials did not constitute cause for dismissal without notice. The court reasoned that the plaintiff did not have any nefarious intent, hide his activities from the defendant's IT department or think he was doing anything improper, and the plaintiff's conduct did not adversely affect the defendant's interests. The court concluded that the plaintiff's "delinquencies" were "not incompatible with a continuation of the employment relationship". The court awarded the plaintiff damages for wrongful dismissal.

5. Settlement Breach by Tweet

Acadia University v. Acadia University Faculty Assn., 2019 CanLII 47957 (ON LA), involved a dispute over a professor's alleged breach of a settlement of the professor's labour relations grievances. The settlement resolved the grievances without any admission of liability or culpability by any of the parties, and required the parties to keep the terms of settlement strictly confidential. Soon after the settlement agreement was signed, the professor began posting comments about the settlement on Twitter, including numerous tweets about "vindication" and "severance pay". The professor continued to tweet in breach of an arbitrator's direction that he comply with the confidentiality requirements of the settlement. The University applied to the arbitrator for an order that it was not required to make any further settlement payment to the professor. The arbitrator held that settlements in labour law are "sacrosanct", and given the professor's repeated and continuing breaches of the settlement agreement, together with the absence of any mitigating circumstance or explanation, the University was not required to make any further settlement payments.

This paper provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.