

## Canadian Internet Law Update – 2018\*

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

This paper summarizes selected developments in Canadian Internet law during 2018. 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

*Hilton Worldwide Holding LLP v. Miller Thomson*, 2018 FC 895, involved an appeal from a decision of the Registrar of Trademarks expunging the registration of the “Waldorf-Astoria” trademark registered for use in association with “hotel services” because there was no physical “Waldorf-Astoria” hotel in Canada. The court confirmed the well-established principle that in order for a trademark to be used in association with services “it is essential some aspect of the services must be offered directly to Canadians or performed in Canada”. The court held that determining whether services are performed in Canada requires a case-by-case assessment and analysis of the scope of the services and the nature and benefits delivered to people physically present in Canada. The court held that the “Waldorf-Astoria” trademark had been used in association with “hotel services”, even though there was no physical hotel operated under that trademark in Canada. The court reasoned as follows: the word “services” should be liberally construed, and could in appropriate cases include “primary, incidental or ancillary” services; the ordinary commercial understanding of “hotel services”, from the perspective of the trademark owner and consumers, included reservation services; people in Canada could take meaningful benefit from online hotel reservation services, including discounts and reward points; and the “Waldorf-Astoria” trademark was displayed on the reservation website accessed by customers in Canada and on emails and booking confirmations received by customers in Canada. The court allowed the appeal and set aside the Registrar’s decision. See also *Dollar General Corp. v. 2900319 Canada Inc.*, 2018 FC 778.

#### 2. Infringing Domain Name

*Royal Pacific Real Estate Group Ltd. v. Dong*, 2018 BCSC 1272, involved a dispute over the defendants’ unauthorized use and infringement of the plaintiffs’ registered “Royal Pacific and design” trademark in connection with a competing real estate agency business. The defendants used confusingly similar trademarks on their website and Facebook page and in emails. The defendants also registered the royalpacific.co domain name and used it for their real estate business website. The court held the defendants liable for trademark infringement and passing off. The court found that the defendants’ use of the royalpacific.co domain name for their website, which included numerous references to aspects of the plaintiffs’ business, “would have caused confusion in the mind of an ‘ordinary hurried consumer’, who could have confused the owner of the website with the [plaintiff]”. The court awarded the plaintiffs \$6,000 in general damages, an injunction prohibiting future infringement and an order transferring ownership of the royalpacific.co domain name to the plaintiffs. The court held that it had jurisdiction to order the domain name transfer pursuant to *Trademarks Act* s. 53.2(1), and reasoned that the order was necessary to protect the plaintiffs’ rights and reduce the risk of further litigation over the use of the domain name.

---

\*Copyright © 2019 Bradley Freedman. All rights reserved. This paper is an abridged version of a chapter in *Annual Review of Law & Practice*, 2019, Continuing Legal Education Society of British Columbia.

## **B. Copyright**

### **1. Amendment to Copyright Act Notice and Notice Regime**

The *Budget Implementation Act, 2018, No. 2* (Bill C-86) amended the *Copyright Act* to prohibit certain information in a notice of claimed copyright infringement delivered pursuant to the “notice and notice” regime set out in *Copyright Act* ss. 41.25 and 41.26. As a result of the amendments, an Internet service provider is not obligated to forward a notice of claimed copyright infringement to an alleged infringer if the notice contains any of the following: (1) an offer to settle the claimed infringement; (2) a request or demand, made in relation to the claimed infringement, for payment or for personal information; (3) a reference, including by way of hyperlink, to such an offer, request or demand; or (4) any other information that may be prescribed by regulation.

### **2. ISP’s Entitlement to Costs under a Norwich Order**

*Rogers Communications Inc. v. Voltage Pictures, LLC*, 2018 SCC 38, involved a proposed reverse class proceeding against unknown defendants engaged in illegal Internet sharing of the plaintiffs’ copyright protected films. The plaintiffs brought an application for a *Norwich* disclosure order requiring Rogers Communications, a non-party Internet service provider, 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 proceeding. The Supreme Court of Canada held as follows: The notice and notice regime established by the *Copyright Act* does not require an Internet service provider (an “ISP”) to disclose to a copyright owner the identity and physical address of a person who is alleged to have committed a copyright infringement. A copyright owner who wishes to obtain that information from an ISP must obtain a *Norwich* disclosure order to compel the ISP to disclose the information. *Copyright Act* s. 41.26(2) prohibits an ISP from charging a fee for complying with the notice and notice regime (except where the Minister has fixed a maximum fee by regulation, which has not yet occurred). An ISP is entitled to its reasonable costs of compliance with a *Norwich* disclosure order, but is not entitled to compensation for costs that the ISP should have incurred in performing its statutory obligations under the notice and notice regime, even if it carries out those obligations only after it has been served with the *Norwich* disclosure order. Those obligations implicitly include: (1) determining, for the purposes of forwarding an infringement notice, who was assigned the impugned IP address at the time of the alleged infringement; (2) taking all steps necessary to verify that the ISP has done so accurately; and (3) taking all steps necessary to verify the accuracy of records that would permit the ISP to identify the name and physical address of the person to whom the infringement notice was forwarded. Those obligations do not require an ISP to actually use the records to determine the name and physical address of the person to whom an infringement notice was forwarded, or to keep the records in a form and manner that would permit a copyright owner or a court to determine that information. Consequently, an ISP is entitled to the reasonable costs of the steps necessary to discern a person’s identity from the accurate records retained by the ISP in compliance with the notice and notice regime. Motions judges should carefully review an ISP’s evidence of costs of compliance with a *Norwich* disclosure order to determine whether the costs are reasonable in light of the ISP’s obligations under the notice and notice regime.

### **3. Link to Website Infringes Copyright**

*Collett v. Northland Art Company Canada Inc.*, 2018 FC 269, involved a dispute between a professional photographer and a gallery that had been authorized to advertise and sell his photographs. The photographer claimed that after his business relationship with the gallery ended, the gallery infringed his copyright and moral rights by continuing to advertise and sell prints of his photographs and by maintaining unauthorized links to his personal website (which included one of the photographs and the photographer’s biography). The court also held that the gallery had infringed the photographer’s copyright in certain photographs by reproducing the photographs on the gallery’s website. The court held that the gallery had infringed the photographer’s copyright in his personal website by maintaining a link from the gallery’s website to the photographer’s website even though the gallery knew that it was not authorized to do so. The court ordered the gallery to pay to the plaintiff \$45,000 statutory damages for copyright infringement, \$10,000 for infringement of moral rights, and \$25,000 punitive damages.

#### 4. Injunction to Stop Facilitating Copyright Infringement

*Bell Canada v. Lackman*, 2018 FCA 42, involved a dispute over the defendant's TVAddons.ag website, which was a repository of both infringing add-ons (which directed users to stream and download copyright protected movies and television shows without authorization from the copyright owners) and non-infringing add-ons (which directed users to legitimate websites). The plaintiff media companies sued the defendant for infringing copyright by communicating and making infringing add-ons available to the public, and by inducing or authorizing users of infringing add-ons to initiate acts of copyright infringement. The plaintiffs obtained an *ex parte* Anton Piller order and an *ex parte* interim injunction against the defendant's operation of the TVAddons.ag website. The injunction was set aside by a motions judge who held that the defendant was an Internet intermediary protected from liability by *Copyright Act* s. 2.4(1)(b). On appeal, the court of appeal held as follows: the motions judge misapprehended the evidence and made palpable and overriding errors; there was "clearly a strong prima facie case" that the defendant, by hosting and distributing infringing add-ons, was infringing copyright in the plaintiffs' content; the defendant's website was designed to facilitate access to infringing material on the Internet, and was therefore not a mere conduit entitled to protection from liability by *Copyright Act* s. 2.4(1)(b); the motions judge erred in failing to consider the plaintiffs' separate claim that the defendant induced and authorized acts of copyright infringement by encouraging users to access infringing content when they would otherwise not have done so; and the motions judge erred in dismissing the plaintiffs' application for an interlocutory injunction. The court of appeal reasoned that an interlocutory injunction was appropriate because there was a serious issue to be tried, the plaintiffs would suffer irreparable harm if the injunction was not granted and the balance of convenience favoured granting an injunction. The court of appeal noted that the defendant's bald assertion that an injunction would cause financial hardship was not supported by any evidence, and in any event was not sufficient to support a finding that the balance of convenience was against granting an injunction. The court of appeal granted the appeal and issued an interlocutory injunction.

### C. Contracts and Electronic Transactions

#### 1. Contract Made by Email

*Hurst Real Estate Service Inc. v. Great Lands Corp.*, 2018 ONSC 4824, involved a dispute over the plaintiffs' entitlement to commission regarding a commercial real estate transaction between the defendant and a buyer introduced by the plaintiffs. The court found that a series of emails between the parties constituted a valid and binding agreement that the defendant would pay to the plaintiffs a commission in respect of the transaction. The court further held that the plaintiffs' claims were not barred by a regulation to the *Real Estate and Business Brokers Act, 2002*, which provides that a claim for commission cannot be brought unless the agreement to pay a commission is in writing and signed by or on behalf of the person who is required to pay the commission. The court held that the emails satisfied the signature requirement because they ended with a typed version of the sender's name, his title and the name of the corporation he represented. The court stated (para. 66): "I am satisfied that in this digital age in which commerce is routinely conducted with the assistance of information technology, this type of electronic signature meets the requirement ... that the offer be 'signed by or on behalf of the person required to pay the commission'".

#### 2. Notice of Resignation by Text Message

*Kasumu v. Musah*, 2018 ABQB 242, involved a shareholders' dispute among physicians who operated a joint medical practice through a company. One of the physicians sent a text message to the personal mobile phone of the company's president/chief executive officer advising that the physician "officially resigned her position as a director ... effective today". A few days later the physician took the position that she had not formally resigned. The company's by-laws provided that a director may resign by "written resignation ... sent or delivered to the company". Similarly, the *Alberta Business Corporations Act* provides that a corporate director may resign by "written resignation" given to the corporation. The court referred to previous decisions holding that a resignation notice could be effectively delivered to a company by means other than delivery to the company's registered office, provided that the notice is "meaningfully communicated" and "capable of objective verification". The court held that the text message constituted a "written" notice within the meaning of the company's by-laws and the *Business Corporations Act*. The court also held that the resignation had been "meaningfully communicated" to the company because it was sent by text message to the president

and shortly thereafter all directors and the company's lawyer were aware of the resignation. For those reasons, the court held that the resignation was effective on the day the text message was received.

### **3. Notice of Termination Delivered by Email**

*Polygon Metalworks Int'l Inc. v. Ellisdon Corp.*, 2018 BCSC 1448, involved a dispute over the termination of a subcontract for the supply of stainless steel for an office tower construction project. The subcontract set out physical addresses for the delivery of notices to the parties, provided that all notices must be in writing and were deemed received on the date of delivery, and set out deemed delivery dates for notices delivered by hand, registered post and regular post. The defendant delivered notices of default and termination to the plaintiff by email. The plaintiff asserted that the notices were invalid because the subcontract did not permit delivery of notices by email. The court held that the email notices were valid and effective when received by the plaintiff. The court reasoned that the subcontract did not prohibit delivery of notices by means other than delivery to the physical addresses of the parties, and therefore did not preclude the parties from delivering notices by email. The court noted that the parties had communicated by email throughout their relationship.

## **D. Internet Defamation**

### **1. Jurisdiction Over Online Defamation Dispute**

*Haaretz.com v. Goldhar*, 2018 SCC 28, involved a defamation dispute over a newspaper article published in print and online by an Israeli newspaper. The plaintiff Canadian businessman owned an Israeli soccer team. The defendant newspaper published, in both print and on the newspaper's Hebrew and English-language websites, an article criticizing the plaintiff's management of the team in a manner that implicated the plaintiff's Canadian business practices and integrity as a Canadian businessman. The article was read by 200 to 300 people in Canada and approximately 70,000 people in Israel. The plaintiff commenced a lawsuit in Ontario claiming damages for libel. The defendant newspaper brought a motion challenging the court's jurisdiction. At the jurisdiction hearing, the plaintiff agreed to limit his damages claims to reputational harm suffered in Canada only, to pay for the costs of Israeli witnesses to travel to Ontario for the lawsuit, and to not commence litigation over the article elsewhere. The motions judge dismissed the newspaper's motion (2015 ONSC 1128), and the defendant appealed. The court of appeal majority dismissed the appeal on the basis that the libel action had significant connections to Ontario, and an Israeli court was not a clearly more appropriate forum (2016 ONCA 515). On appeal by the newspaper, the Supreme Court of Canada, in a complicated three-one-one-one-three split decision, allowed the appeal and ordered the Ontario action stayed in favour of a lawsuit in Israel.

The Supreme Court majority explained that: (1) jurisdiction *simpliciter*, which exists where there is a "real and substantial connection" between the chosen forum and the subject matter of the litigation, prioritizes order, stability and predictability by relying on objective connecting factors for the assumption of jurisdiction; and (2) the *forum non conveniens* analysis tempers any potential rigidity in the rules governing assumption of jurisdiction and assures fairness to the parties and the efficient resolution of the dispute by adopting a case-by-case approach to determine whether an alternative jurisdiction is "clearly more appropriate" based on considerations of fairness and efficiency. The majority cautioned that presumptive connecting factors for jurisdiction *simpliciter* were not irrebuttable, and that motions judges should be particularly attuned to concerns about fairness and efficiency at the *forum non conveniens* stage in Internet defamation cases. The majority held that the Ontario court had jurisdiction *simpliciter* because there was a presumptive connecting factor – the situs of the Internet-based defamation tort was in Ontario, where the defamatory statements were read, accessed or downloaded – and the newspaper did not rebut that presumption by establishing that it was not reasonable to expect that the newspaper would be called to answer defamation proceedings in Ontario. The majority considered various factors – comparative convenience and expense for the parties, comparative convenience and expense for witnesses, legitimate juridical advantage, fairness, enforcement and applicable law – and held that the newspaper had established that Israel was clearly a more appropriate forum. In making that finding, the majority discounted the plaintiff's undertaking to seek damages for reputational harm in Canada only, finding that it did not narrow the scope of the plaintiff's pleadings or preclude him from bringing a future action in Israel.

The dissenting minority held that the Ontario court had jurisdiction *simpliciter*, and the relevant factors in the *forum non conveniens* analysis did not meet the test of showing that Israel was a "clearly more appropriate

forum” than Ontario. The minority emphasized that fairness militated in favour of the plaintiff being able to vindicate his reputation in the courts of Ontario, where he lived and maintained his business and where the sting of the article’s comments was felt by him.

## **2. Fair Comment Defence for Internet Defamation**

*Walsh Energy Inc. v. Better Business Bureau of Ottawa-Hull Inc.*, 2018 ONCA 383, involved a defamation dispute over the defendant’s publication, on its business-rating website, of a D– rating of the plaintiff’s residential heating and air conditioning business. The rating was based on one unresolved customer complaint. The trial judge (2012 ONSC 5819) dismissed the plaintiff’s claim on the basis that the rating was not defamatory and was protected by the defence of fair comment. On appeal, the divisional court (2016 ONSC 1606) held that the D– rating was defamatory of the plaintiff and was not protected by the fair comment defence. On further appeal, the court of appeal held that the divisional court erred by not finding that the defamatory D– rating was protected as fair comment. The court of appeal held that the fair comment defence applied because the D– rating was an opinion on a matter of public interest that was based on fact and could honestly have been expressed on the proven facts, and the plaintiff had failed to prove that the defendant was actuated by malice.

## **3. Damages for Internet Defamation**

*Rutman v. Rabinowitz*, 2018 ONCA 80, involved a dispute among long-time business associates that gave rise to a serious, sustained and baseless Internet defamation campaign designed to harm the plaintiff’s personal and professional reputations. The campaign involved fraudulent emails and Internet postings of numerous malicious and entirely false defamatory allegations. The defamatory statements were “unrelenting, insidious and reprehensible”. The trial judge (2016 ONSC 5864) held the two individual defendants and their corporation to be jointly and severally liable for the defamation, and awarded the plaintiff general, aggravated and punitive damages totaling \$700,000. On appeal, the court of appeal held that the trial judge correctly found the individual defendants jointly liable for the defamation based on “concerted action liability”, and the corporate defendant vicariously liable for the defamation because it was associated with the defamatory statements and was “an authorized vehicle” for the misdeeds of the individual defendants. The court of appeal also held that the trial judge did not err in assessing damages, because the damages awards were rationally related to the underlying objectives of retribution, deterrence and denunciation. The court of appeal noted (para. 68) that “the pernicious effect of defamation on the Internet ... distinguishes it, for the purposes of damages, from defamation in another medium”; the traditional factors to be considered in determining general damages for defamation “must be examined in light of the Internet context of the offending conduct”; and damages for Internet defamation must be assessed in the context of the “unique and somewhat insidious nature of [I]nternet defamation” and in light of the fact that the defamatory statements at issue were “instantly available to an unknown number of recipients” (para. 70). The defendants’ application for leave to appeal to the Supreme Court of Canada was dismissed (*Saul Rabinowitz v. Ronald Rutman*, 2018 CanLII 73625 (SCC)).

## **4. Disgruntled Customer Liable for Defamatory Social Media Posts**

*Hee Creations Group Ltd. v. Chow*, 2018 BCSC 260, involved a dispute over the defendant’s disparaging social media comments about the plaintiff’s wedding services business. The plaintiff’s business catered primarily to Chinese-speaking customers. The defendant hired the plaintiff to provide various wedding services, including a photographer. The defendant was unhappy with the wedding photographs, and refused to pay for the plaintiff’s services. Over a 12-month period, the defendant published on various English and Chinese language blogs, forums and social media sites numerous disparaging comments about the plaintiff and its services. The dispute over the unpaid fees was resolved through a small claims action, in which the defendant’s claims were dismissed and the plaintiff’s counterclaim for fees was allowed in full. After the small claims court judgment was issued, the defendant published an apology on various social media sites. The plaintiff was not able to recover from the harm caused by the disparaging comments, and ceased doing business. The court held that the disparaging comments were defamatory and published with malice. The court found that the defamatory comments had a devastating effect on the plaintiff’s business. In assessing damages, the court noted that “[w]ithin a particular cultural community, the damage caused by defamatory statements can have a much more pervasive and far-reaching impact than at large”, and that Internet platforms “are an extremely powerful medium” that provide “widespread, instantaneous and permanent

dissemination of information, whether true or not” (para. 110). With respect to punitive damages, the court stated that the defendant “and others who think it is acceptable to use the Internet as a vehicle to vent their frustrations, must be given the message that there will be consequences if their publications are defamatory” (para. 132). The court ordered the defendant to pay the plaintiff \$75,000 general damages, \$15,000 aggravated damages, and \$25,000 punitive damages.

## **5. Limitation Period for Defamatory Newspaper Articles**

In *Darren John v. Alex Ballingall*, 2018 CanLII 43780, the Supreme Court of Canada dismissed an application for leave to appeal from a decision of the Ontario Court of Appeal (2017 ONCA 579) holding that the statutory notice and limitation periods in the *Libel and Slander Act* (Ontario) for libel “in a newspaper” applied to an alleged defamatory article published on the Toronto Star newspaper’s website.

## **6. Damages and Injunction for Defamation**

*Nazerli v. Mitchell*, 2018 BCCA 104, leave to appeal refused 2018 CanLII 73621 (SCC), on appeal from 2016 BCSC 810, 2016 BCSC 2085 and 2016 BCSC 2424, involved a dispute over defamatory articles published on the “Deep Capture” website and republished on other websites. The trial judge held that the defendants engaged in a calculated and ruthless defamation campaign to inflict as much damage on the plaintiff’s reputation as they could achieve, which caused the plaintiff significant harm. The trial judge awarded the plaintiff \$400,000 general damages, \$500,000 aggravated damages, \$250,000 punitive damages and \$55,000 special damages. The trial judge also granted a permanent injunction restraining the defendants from “publishing on the Internet or elsewhere any defamatory words concerning the plaintiff”. On appeal, the court of appeal upheld the trial judge’s decision but varied the remedies. The court of appeal held that the trial judge’s award of aggravated damages was inordinately high, and reduced the award to \$200,000. The court of appeal also held that the injunction, which had world-wide effect, should be limited to the words that were found by the trial judge to be defamatory, and should give the defendants liberty to apply to vary the injunction “as circumstances may require”.

## **E. Canada’s Anti-Spam Legislation (“CASL”)**

### **1. Regulatory Enforcement**

In 2018, the Canadian Radio-television and Telecommunications Commission (CRTC) announced two voluntary undertakings to settle CASL investigations and issued a CASL enforcement decision.

- In January 2018, the CRTC accepted an undertaking by Ancestry Ireland Unlimited Company to settle alleged CASL violations regarding the sending of promotional emails without a CASL-compliant unsubscribe mechanism. Ancestry allegedly sent its customers two kinds of promotional emails, each with its own unsubscribe management system, so that it was not possible for a customer to use a single operation to unsubscribe from both kinds of promotional emails. The lack of a single unsubscribe operation allegedly did not comply with the CASL requirement for an easily performed unsubscribe mechanism that allows a recipient to unsubscribe from receiving any future commercial electronic messages.
- In May 2018, the CRTC announced that the companies operating the 514-BILLETS ticket resale business agreed to pay \$100,000 as part of a voluntary settlement of alleged CASL violations regarding the sending of text messages without the recipients’ consent and without prescribed information about the message sender. The undertaking was the first settlement of an investigation regarding the sending of text messages to mobile devices.
- In July 2018, the CRTC issued notices of violation imposing penalties totaling \$250,000 against two online advertising businesses for allegedly violating CASL by aiding their anonymous customers to distribute online ads that surreptitiously installed malicious computer programs in violation of CASL’s computer program rules. According to the CRTC’s announcement and investigation summary, the two businesses were warned that their services were being used to distribute malvertising, but they did not implement safeguards to prevent those activities.

## 2. Regulatory Guidance

In November 2018, the CRTC issued *Compliance and Enforcement Information Bulletin CRTC 2018-415* titled “Guidelines on the Commission’s approach to s. 9 of Canada’s anti-spam legislation (CASL)” to provide guidance regarding CASL s. 9, which imposes liability on persons who “aid, induce, procure or cause to be procured” a CASL violation. The Bulletin explains the CRTC’s approach to s. 9, includes examples of organizations to which s. 9 could apply and activities that could result in non-compliance, and provides guidance for organizations seeking to manage associated risks. The Bulletin explains the CRTC’s view that CASL s. 9 imposes strict liability on persons who assist a CASL violation, and that businesses that provide products or services that could be used to commit CASL violations must implement proactive measures to prevent identified risks, even if that means going beyond industry standards.

## F. Criminal Law

### 1. Warrantless Seizure of Shared Home Computer Violates Charter Rights

*R. v. Reeves*, 2018 SCC 56, involved a challenge to the admissibility of evidence found as a result of a warrantless seizure of a shared household computer and the subsequent search of the computer without a valid warrant. A police officer came to the accused’s family home after the accused’s spouse reported finding child pornography on the home computer she shared with the accused. The computer was taken by the police with the consent of the accused’s spouse but without a warrant. The police failed to report the seizure of the computer to a justice, and held the computer for more than four months before searching it. When the police finally obtained a search warrant (which was later held invalid) and searched the computer, they found child pornography. The accused was charged with possession and accessing child pornography. The accused applied to exclude the computer-related evidence on the basis that it was obtained in violation of his Charter rights. The trial judge agreed, and excluded the evidence. The accused was acquitted. The court of appeal allowed the crown’s appeal, set aside the exclusionary order and ordered a new trial. The Supreme Court of Canada allowed the accused’s appeal, held that the computer-related evidence was properly excluded and restored the acquittal entered at trial.

The Supreme Court of Canada, in a 7-1-1 split decision, held that the police infringed the accused’s Charter rights when they took the shared computer from his home without a warrant because the accused had a reasonable expectation of privacy in the computer, and the accused’s spouse’s consent did not nullify the accused’s reasonable expectation of privacy or operate to waive his Charter rights in the computer. The court majority reasoned that a police seizure of a computer infringes the computer user’s privacy interests because it deprives the user of control over data in the computer, including the opportunity to delete the data, and preserves the data for future state inspection. The court majority further reasoned that joint ownership and shared control over the home computer diminished but did not eliminate the accused’s reasonable expectation of privacy. The court majority held that waiver of Charter rights by the accused’s spouse did not constitute a waiver on behalf of the accused—“waiver by one rights holder does not constitute waiver for all rights holders” (para. 52). The court majority further held that the “unique and heightened privacy interests in personal computer data clearly warrant strong protection, such that specific, prior judicial authorization is presumptively required to seize a personal computer from a home” (para. 35). The court majority stated: “because someone is always likely to have a reasonable expectation of privacy in a personal computer, the taking of a personal computer without a warrant and without valid consent will constitute a presumptively unreasonable seizure” (para. 56). The court majority held that there were serious Charter breaches throughout the investigative process, and the admission of the evidence would bring the administration of justice into disrepute.

### 2. Production Order Against Foreign Company with Virtual Presence in Canada

*British Columbia (Attorney General) v. Brecknell*, 2018 BCCA 5, involved an application pursuant to *Criminal Code* s. 487.014(1) for an order that Craigslist Inc. produce documents located outside Canada to a peace officer in British Columbia for use in connection with an investigation into alleged serious criminal offences committed by use of the Internet in British Columbia. The documents related to a Craigslist posting made in British Columbia. Craigslist provided Internet advertising services to users in British Columbia, but had no physical presence in Canada and was not a registered company in British Columbia. The application judge (2017 BCSC 460) held that the court did not have jurisdiction to issue the order against Craigslist. On

appeal, the court of appeal held that the court had jurisdiction to issue the order against Craigslist because Craigslist was located in Canada for the purpose of the *Criminal Code* section. The court reasoned that corporations can conduct business in multiple jurisdictions without the need for a physical presence in the jurisdictions, and that a virtual presence in British Columbia was sufficient to provide the jurisdictional foundation for the issuance of the production order without having impermissible extraterritorial consequences. The court stated: "... in the Internet era it is formalistic and artificial to draw a distinction between physical and virtual presence. ... To draw on and rely on such a distinction would defeat the purpose of the legislation and ignore the realities of modern day electronic commerce" (para. 40). The court also held that issuing the production order against Craigslist would not have impermissible extraterritorial effects. The court reasoned that "legislation must be interpreted in light of contemporary technology and take into account the changed technological environment to which it must be applied. That imperative applies in the context of criminal investigation in the digital world and colours the analysis of whether a particular investigative technique has impermissible extraterritorial effects".

## **G. Miscellaneous**

### **1. Injunction Prohibiting Global Internet Search Results**

*Equustek Solutions Inc. v. Jack*, 2018 BCSC 610, involved an application to vary 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 developed through theft of the plaintiffs' trade secrets. When the Supreme Court of Canada previously affirmed the injunction (2017 SCC 34), the majority of the court held that Google could apply to vary the injunction on the basis of evidence that the injunction would require Google to "violate the laws of another jurisdiction, including interfering with freedom of expression". After the Supreme Court of Canada issued its decision, Google commenced proceedings in a U.S. District Court and obtained an unopposed order that the Canadian injunction was unlawful and unenforceable in the United States. The U.S. District Court held that the Canadian injunction was contrary to the United States *Communications Decency Act* and threatened free speech on the global Internet. Google then applied to the British Columbia Supreme Court to vary the injunction based on the U.S. District Court's decision. The British Columbia Supreme Court dismissed Google's application. The court held that the U.S. District Court's decision did not establish that the injunction required Google to violate American law. The court stated: "The effect of the U.S. order is that no action can be taken against Google to enforce the injunction in U.S. courts. That does not restrict the ability of this Court to protect the integrity of its own process through orders directed to parties over whom it has personal jurisdiction" (para. 22). The court held that "there is no suggestion that any U.S. law prohibits Google from de-indexing those websites, either in compliance with the injunction or for any other reason. ... A party being restricted in its ability to exercise certain rights is not the same thing as that party being required to violate the law" (para. 20). The court further held that Google had not demonstrated that the injunction violated core American values. The court rejected Google's additional arguments that other changed circumstances justified setting aside the injunction.

### **2. Tort of Public Disclosure of Private Facts**

*Jane Doe 72511 v. Morgan*, 2018 ONSC 6607, involved a dispute over physical assaults and the unauthorized posting of a sexually explicit video of the plaintiff on a pornographic website. The plaintiff and her boyfriend were unmarried parents of an infant, and lived together in the boyfriend's parents' home. The boyfriend was violent and abusive to the plaintiff. The plaintiff reported a violent incident to the police, and the boyfriend was arrested and convicted of assault. The boyfriend posted the sexually explicit video of the plaintiff as revenge for the plaintiff calling the police, and threatened to post nude photos of the plaintiff if she took any legal steps against him. The plaintiff had consented to the making of the video, but not to its disclosure to other people or its posting on the Internet. The plaintiff commenced the lawsuit against the boyfriend and his parents seeking damages for assault and battery and for public disclosure of private facts. The boyfriend and his parents did not defend the lawsuit, and the plaintiff applied for default judgment.

The court held that it was appropriate to provide the plaintiff with a civil remedy for invasion of her privacy by adopting the tort of public disclosure of private facts into the law of Ontario. The court relied on the reasoning in *Jones v. Tsige*, 2012 ONCA 32, and *Jane Doe 464533 v. N.D.*, 2016 ONSC 541. The court described the



tort as follows: “To establish liability, the plaintiff must ... prove that: (a) the boyfriend publicized an aspect of the plaintiff’s private life; (b) the plaintiff did not consent to the publication; (c) the matter publicized or its publication would be highly offensive to a reasonable person; and (d) the publication was not of legitimate concern to the public” (para. 99). The court reasoned that the adoption of the tort was not incompatible with any statutory scheme for the protection of privacy rights in Ontario, and was consistent with and complemented the *Criminal Code* offence of publication of an intimate image without consent. The court explained (at paras. 94 and 94) that the adoption of the tort was “a constructive, incremental modification of existing law to address a challenge posed by new technology” and “an appropriate, proportionate legal response to a growing problem enabled by new technology”.

The court held that the boyfriend was liable for assault and battery and for public disclosure of private information. The court held that the boyfriend’s parents were not liable for the boyfriend’s unauthorized posting of the video because they did not know about the video and the incident was not reasonably foreseeable. As compensation for posting the video, the court ordered the boyfriend to pay to the plaintiff \$50,000 in general damages, \$25,000 in aggravated damages, and \$25,000 in punitive damages. The court also ordered the boyfriend to destroy any other nude, intimate or sexually explicit images or recordings of the plaintiff, and prohibited the boyfriend from disclosing those images or records.

### **3. Nude Selfies Do Not Breach a Good Morals Clause**

*Zigomanis v. 2156775 Ontario Inc.*, 2018 ONCA 116, involved a dispute over the termination of a contract for the plaintiff athlete’s paid endorsement and promotion of the defendant drink company’s energy drinks. Before the contract was signed, the athlete took photographs of his naked body (front and back, but not showing his face) and sent the photographs to his girlfriend. After the contract was signed, unknown individuals obtained and published the photographs on the Internet. The drink company terminated the contract on the basis that the athlete had breached a contractual morals clause, which allowed the company to terminate the contract if the athlete “commits any act which shocks, insults, or offends the community, or which has the effect of ridiculing public morals and decency”. The athlete sued for wrongful termination. The trial judge (2016 ONSC 7053) held that the morals clause was not applicable. The court of appeal dismissed the company’s appeal on the basis that the trial judge did not make “a palpable and overriding error in failing to find that sharing nude photographs within an intimate relationship would shock the conscience of the community” (para. 7). The court stated: “The trial judge’s conclusion that the community conscience would not be shocked was his to make. It was rooted, appropriately, in the timeless human practice of sharing intimate information within relationships, the inherent expectation of privacy when doing so, and the public policy reflected in recent legislation protecting the privacy of such communications in the internet age” (para. 9). The company’s application for leave to appeal to the Supreme Court of Canada was dismissed (2018 CanLII 105392 (SCC)).

### **4. Deceptive Marketing Practices—Influencer Marketing**

The Competition Bureau’s *Deceptive Marketing Practices Digest, Volume 4*, discussed the application of the *Competition Act* provisions regarding advertising and marketing to “influencer marketing” – the use of online platforms (e.g. social networks, blogs and photo-sharing apps) by popular individuals to influence the choices by their followers. The Digest included an “Influencers’ checklist” for posting reviews and opinions on social media, and noted that social media influencers should clearly disclose any material connections they have with the companies whose products or services they feature, and their stated online reviews, testimonials and endorsements must be genuine and based on actual experience. The Digest also included an “Advertisers’ checklist” for advertisers who engage social media influencers, and noted that advertisers or their agents should be careful to ensure that their influencer marketing complies with *Competition Act* requirements. The Digest encouraged advertisers and influencers to consult the *Disclosure Guidelines* for influencer marketing published in September 2018 by the Influencer Marketing Steering Committee.

---

**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.**