March 29, 2016

ARTICLE

Canadian Internet Law Update - 2015

This paper summarizes selected developments in Canadian Internet law during 2015. Internet law is a vast area that continues to develop rapidly. Reference to current legislation, regulatory policies, and guidelines and case law is essential for anyone addressing these issues in practice.[1]

Trademarks

Keyword Advertising

Vancouver Community College v. Vancouver Career College (Burnaby) Inc., 2015 BCSC 1470, involved a dispute over the defendant's advertising and promotion of educational services in competition with the plaintiff's educational services. The plaintiff claimed that the defendant misrepresented the defendant's educational services as those of the plaintiff by using certain terms (including the plaintiff's trade name) as keywords for advertising on Internet search sites and by using the "VCCollege.ca" domain name. The plaintiff alleged passing off, and argued that the defendant's keyword advertising caused initial interest confusion. The court held that, for the purpose of assessing a likelihood of confusion, the relevant "first impression" occurs when an individual using an Internet search site accesses a listed website. The court reasoned that an Internet user understands that it is necessary to view a website to determine who owns the site, and it is at that point when the relevant first impression is made. The court concluded that the defendant's use of the plaintiff's trade name as advertising keywords did not cause confusion. The court also held that the evidence did not support the plaintiff's allegation that the defendant's use of the "VCCollege.ca" domain name caused confusion.

Trademarks in Metatags

Red Label Vacations Inc. v. 411 Travel Buys Ltd., 2015 FCA 290, dismissing appeal from 2015 FC 19, involved a dispute over the defendant's limited duration use in its travel business website of metatags (titles, descriptions, and keywords, including the plaintiff's trademarks) inadvertently copied from the plaintiff's travel business website. The plaintiff claimed that the defendant's use of the copied metatags constituted copyright infringement (discussed below), trademark infringement, passing off, and depreciation of goodwill in registered trademarks.

The trial judge held that the use of the copied metatags, which were not visible to website users, did not create a likelihood of confusion required for a successful trademark infringement or passing off claim. The trial judge held that the concept of "initial interest confusion" was not applicable because, while metatags may influence Internet search results, those results present searchers with a choice of links to websites, rather than directing searchers to a particular website, and each searcher retains the ability to choose which website to access and which website to use to purchase goods or services. The trial judge reasoned that trademark infringement and passing off require confusion as to the source of the goods or services advertised on a website. For those reasons, the trial judge held that the use of a competitor's trademark or trade name in metatags does not, by itself, constitute a basis for the likelihood of confusion required for passing off or trademark infringement. The trial judge noted that the defendant's website was clearly identified, and there was no likelihood of deception as to the source of the advertised services. The trial judge held that use of trademarks in non-visible metatags did not support a finding of depreciation of goodwill. The plaintiff appealed.

The court of appeal dismissed the appeal, primarily on the basis that the plaintiff failed to demonstrate that the trial judge made any palpable and overriding error in his determinative findings. Nevertheless, the court of appeal attempted to limit the scope of the trial judge's ruling regarding metatags. The court majority expressed the view (at para. 22) that "...in some situations, inserting a registered trade-mark (or a trade-mark that is confusing with a registered trademark) in a metatag may constitute advertising of services that would give rise to a claim for infringement...". The concurring court of appeal justice stated (at para. 45): "The extent to which a trademark may be used in metatags without infringing the trademark is, of necessity, fact specific. These reasons ought not to be read as endorsing the Judge's remarks relating to 'initial interest confusion' or as endorsing every alternate basis on which the Judge dismissed the action".

Infringing Domain Name

British Columbia Recreation and Parks Assn. v. Zakharia, 2015 BCSC 1650, involved a dispute arising from the termination of the defendant's membership in the plaintiff Association. The defendant used the Internet to malevolently attack and defame the plaintiff and its chief executive officer. The defendant also registered and used the Internet domain name BCfit.ca, which incorporated the plaintiff's registered trademark BCFIT, for a website used to criticize the plaintiff association. The plaintiff sued for defamation, injurious falsehood, conspiracy to injure, false representations to the public, trademark infringement, and passing off. The plaintiff was successful in all of its claims. Regarding the trademark infringement and passing off claims, the court held that the defendant had used the BCfit.ca domain name to misrepresent and confuse Internet users and to create confusion about the plaintiff and its events. The court awarded the plaintiff $18,000 as damages for passing off and trademark infringement and ordered the defendant to transfer the infringing domain name to the plaintiff.

Copyright

Copyright Act Amendments — Notice and Notice Regime

Copyright Act, ss. 41.25, 41.26 and 41.27(3), which implement a "notice and notice" regime for Internet copyright infringement, came into force on January 2, 2015. The regime provides a mechanism for copyright owners to give a prescribed form of notice of Internet-related copyright infringement claims to certain Internet intermediaries (Internet service providers, digital memory/storage providers, and search engine providers), who are required to respond to a notice in a specified manner or face liability.

Tariff 24 Royalties for Ringtone Downloads

Rogers Communications Partnership v. Society of Composers, Authors and Music Publishers of Canada, 2015 FC286, involved a renewed challenge to the validity of Tariff 24 established by the Copyright Board of Canada, which requires the payment of royalties in respect of ringtone downloads to the defendant society (which collects and distributes royalties for public performances of works on behalf of composers, authors, and publishers). The plaintiffs had previously unsuccessfully challenged the Tariff, and had paid royalties under the Tariff for many years. After the Supreme Court of Canada determined in 2012 that the Internet delivery of downloads of musical works and downloads of video games containing musical works did not constitute the communication of those works to the public by telecommunication (*Rogers Communications Inc. v. Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 35 and *Entertainment Software Association v. Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 34), the plaintiffs stopped paying royalties and renewed their challenge to the Tariff. Following the Supreme Court decisions, the court held

that the Internet transmission of a ringtone download constitutes a reproduction, rather than a communication, of the ringtone. For that reason, the court held that the Tariff became unenforceable after the 2012 Supreme Court of Canada decisions, but the defendant society was not required to refund royalties paid before the Supreme Court of Canada decisions.

Copied Metatags

Red Label Vacations Inc. v. 411 Travel Buys Ltd., 2015 FCA 290 dismissing appeal from 2015 FC 19, involved a dispute over the defendant's limited duration use in its travel business website of metatags (titles, descriptions, and keywords) inadvertently copied from the plaintiff's travel business website. The plaintiff claimed that the defendant's use of the copied metatags constituted copyright infringement as well as trademark infringement, passing off and depreciation of goodwill in registered trademarks (discussed above). The trial judge held that the plaintiff's metatags were not sufficiently original to be protected by copyright, there had not been a substantial copying in any event (the copied metatags were from only 48 pages of approximately 180,000 pages of the plaintiff's website), and the innocent infringement would have justified only injunctive relief. The court of appeal dismissed the plaintiff's appeal on the basis that the plaintiff failed to demonstrate that the trial judge made any palpable and overriding error in the determinative finding that the plaintiff's metatags were not sufficiently original to be protected by copyright.

Circumvention of Technological Protection Measures

1395804 Ontario Ltd. (Blacklock's Reporter) v. Canadian Vintners Assn., 2015 CanLII 65885 (ONSCSM), involved a small claims court lawsuit over the defendant's unauthorized access to and distribution of the plaintiff's paywall-protected article available online to subscription customers only. The article was of interest to the defendant, but instead of paying a modest subscription fee for the article the defendant obtained a copy of the article from a paying subscriber, contrary to the plaintiff's website terms and conditions of use. The court held that the defendant had obtained a copy of the article in violation of *Copyright Act* s. 41.1(1), which prohibits circumvention of a technological protection measure (the paywall) that controls access to a copyright-protected work. The court held that the defence of fair dealing was not available to the defendant because it obtained a copy of the article in violation of *Copyright Act* s. 41.1(1) and in circumstances in which the dealing was not "fair". The court awarded the plaintiff compensatory damages equivalent to a one-year subscription for an institutional licensee ($11,470), $2,000 as punitive damages, interest, and costs.

Contracts

Email Notice of Contract Termination

Muhammad v. Canlanka Ventures Ltd., 2015 ABQB 145, involved a dispute over the defendants' refusal to complete a residential property transaction. The defendants asserted that an email exchange had terminated the transaction, and relied on the *Electronic Transactions Act* (Alberta) to support the argument that termination notice by email was valid. The court rejected the defendants' assertion on the basis that the substance of the emails did not terminate the transaction. The court also held that an email could not qualify as a valid termination notice under the purchase contract, which expressly specified that contractual notices must be in writing and delivered in person or delivered or faxed to a specified address. The court expressed doubt that the electronic equivalency provisions of the Act were applicable because s. 8 of the Act provides that consent is necessary in order to provide or accept information or a record in electronic form and it was not reasonable to infer consent to email notices where the relevant contract contains a clear notice provision that does not contemplate notice by email.

Sponsorship Agreement Made by Emails

Vancouver Canucks Limited Partnership v. Canon Canada Inc., 2015 BCCA 144, dismissing appeal from 2013 BCSC 866, involved a dispute over an alleged sponsorship agreement. The parties engaged in negotiations for the renewal of an equipment supply agreement and a related sponsorship agreement through discussions confirmed by email correspondence that referred to the terms of the previous agreement between the parties. The email correspondence did not state that there would not be a binding agreement until formal contract documents were signed. The parties completed the business discussions and the plaintiff fully activated the defendant's sponsorship benefits. The parties then began negotiating the written contracts and signed a written equipment supply contract. The parties disagreed over the termination provisions of the sponsorship contract, and the defendant ended the negotiations taking the position that there was no binding sponsorship agreement. The plaintiff sued the defendant for breach of contract, alleging that a binding sponsorship agreement was formed through email correspondence. The defendant argued that the emails were an incomplete and unenforceable agreement to agree that was conditional on the negotiation and execution of a written contract. The defendant also argued that its representative who sent the emails did not have authority to bind the defendant. The trial judge rejected the defendant's arguments and held that there was a binding sponsorship agreement created by email. On appeal, the court of appeal held that there was an evidentiary basis for the trial judge's critical findings: a reasonable bystander would conclude the parties intended to be bound by the terms of the emails; the emails, by reference to the previous agreements, included all essential terms for the sponsorship agreement; and the resulting sponsorship agreement was not conditional on subsequent review and approval.

Cancelled Online Order Due to Pricing Error

Faucher v. Costco Wholesale Canada Ltd., 2015 QCCQ 3366, involved a dispute over the defendant retailer's refusal to accept an online order for erroneously priced computers. The plaintiff ordered ten computers for the incorrectly advertised price of $2 each (the real price ought to have been approximately $1,000). The next day the defendant sent to the plaintiff a notice cancelling the order and advising that the plaintiff's credit card had not been charged. The defendant relied on its website terms and conditions, accessible through a link at the bottom of each webpage, which expressly permitted the defendant to cancel an order if the online price was incorrect. The court held that, due to the website terms and conditions, the defendant could not be compelled to accept the order, and that the advertised price was an obvious error that vitiated the defendant's consent to form a contract. The court further held that the defendant's website advertisement, which was viewed by consumers without solicitation, constituted a proposal rather than an offer to form a distance contract governed by the Québec *Consumer Protection Act*. The court further held that the defendant had not engaged in misleading advertising because the defendant did not intend to deceive and the plaintiff was not misled by the obviously incorrect pricing. The court dismissed the plaintiff's claims and ordered the plaintiff to pay the defendant's costs.

Privacy and Personal Information Protection

Digital Privacy Act

The Canadian government enacted the *Digital Privacy Act*, which makes a number of important changes to the *Personal Information Protection and Electronic Documents Act*, including adding provisions regarding disclosure of personal information in a business transaction, data breach notification and record-keeping requirements, employee information and work product information exceptions, and additional powers for the Privacy Commissioner to enter into enforceable compliance agreements. One of the most significant changes is a new, additional requirement for “valid consent” to the collection, use, and disclosure of personal information. Some of the amendments came into force on June 18, 2015, while others (including data breach notification and record-keeping requirements) will not come into force until a later date yet to be fixed.

Proposed Class Action for Breach of Privacy

Douez v. Facebook, Inc., 2015 BCCA 279, involved an application for certification of a class proceeding against Facebook, Inc. for alleged violations of the statutory privacy tort created by the *Privacy Act* (British Columbia) resulting from Facebook's "Sponsored Stories" program. Facebook challenged the court's jurisdiction on the basis that the Facebook Terms of Use specified that claims by users are governed by California law and must be adjudicated in California courts. The chambers judge rejected Facebook's challenge to the court's jurisdiction primarily on the basis that *Privacy Act,* s. 4 gave the British Columbia Supreme Court exclusive jurisdiction to hear claims in respect of the statutory privacy tort, and that if the court declined jurisdiction the plaintiff would have no other forum to bring that claim. The chambers judge certified the class proceeding. Facebook appealed.

The court of appeal allowed the appeal on the basis that the chambers judge erred in her interpretation of *Privacy Act*, s. 4. The court of appeal reasoned that the *Privacy Act*, when interpreted to give effect to the principle of territoriality, did not exclude the jurisdiction of foreign courts to consider *Privacy Act* claims and was not intended to render void a contractual forum selection clause that might deprive British Columbia residents of the right to bring *Privacy Act* claims in the British Columbia Supreme Court. The court of appeal held that the plaintiff had not shown strong cause to not enforce the contractual forum selection clause. Consequently, the court of appeal held that the forum selection clause should be enforced and the action stayed.

Proposed Class Action for Breach of Privacy

Condon v. Canada, 2015 FCA 159, involved an application for certification of a class proceeding arising from the loss of a computer hard drive containing the personal information of approximately 583,000 individuals relating to their participation in the Canada Student Loans Program. The motions judge certified the class proceeding for various causes of action, but not for claims for negligence or breach of confidence because the judge determined that those claims would fail for lack of compensable damages (see 2014 FC 250). The court of appeal held that the motions judge erred by evaluating the merits of the claims based on the evidence adduced in support of the motion rather than on the facts as pled, including "costs incurred in preventing identity theft" and "out-of-pocket expenses". The court of appeal granted the appeal and ordered the claims for negligence and breach of confidence be included in the class proceeding.

Court Jurisdiction over Data Breach Lawsuit

Zuckerman v. Target Corporation, 2015 QCCA 1809 granting appeal from 2015 QCCS 1285, involved a putative class action against Target Corporation for damages resulting from a 2013 cyber-attack in the United States that resulted in the theft of the personal information of millions of customers in the United States and Canada. The defendant applied to dismiss the plaintiff's certification application on the basis that Québec courts lacked jurisdiction. The motions judge granted the application reasoning that the defendant had not committed any fault in Québec (because the data breach occurred in the United States and related to customer data collected in the United States) and the litigation did not involve any activities by the defendant in Québec. The plaintiff appealed. The court of appeal held that the motions judge erred because the plaintiff's alleged harm and expense suffered in Québec were sufficient to give Québec courts jurisdiction over the claim. The court of appeal further held that the motions judge erred by considering circumstances (including the magnitude of the plaintiff's alleged harm, which the motions judge characterized as "ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept") that were irrelevant to the jurisdiction issue, and were more appropriate for an application to decline jurisdiction or to certify the proposed class. The court of appeal granted the appeal, but reserved the defendant's right to argue that the court ought to decline jurisdiction on the basis of *forum non conveniens*.

Regulatory Proceedings Regarding Targeted Advertising

The Office of the Privacy Commissioner of Canada issued *PIPEDA Report of Findings #2015-001* regarding Bell's targeted online advertising program, which delivered targeted advertising to Bell customers based on their Internet browsing activities and other account information. The Office of the Privacy Commissioner of Canada found that the program did not comply with the *Personal Information Protection and Electronic Documents Act* and set out a number of criteria that needed to be met, including providing proper notices to customers about the program, obtaining meaningful and valid opt-in consent due to the sensitive nature of the collected information, and the proper implementation of withdrawals of consent. Bell argued that opt-in consent was not required, and relied on *Privacy and Online Behavioral Advertising Guidelines* previously issued by the Office of the Privacy Commissioner of Canada. The Finding clarified that Bell's advertising program went beyond the type of personal information and advertising contemplated by those guidelines.

Regulatory Guidance

Privacy Commissioners issued guidance for compliance with Canadian personal information protection laws in connection with Internet activities, including the following:

- Privacy Commissioner of Canada — *Collecting from kids? Ten tips for services aimed at children and youth*, to assist organizations that collect, use, and disclose information about youth in connection with online services.
- Privacy Commissioner of Canada — *Interpretation Bulletin — Safeguards*, to provide guidance for compliance with statutory obligations to safeguard personal information.
- Privacy Commissioner of Canada — *Privacy and Cyber Security, Emphasizing privacy protection in cyber security activities*, to assist organizations in balancing the tensions between privacy and cyber security measures.
- Privacy Commissioners of Canada, Alberta, and British Columbia — *Is a bring your own device (BYOD) program the right choice for your organization?*, to assist organizations in determining whether and how to implement a BYOD program that effectively protects an organization's information and respects the privacy rights of employees and customers.
- Information and Privacy Commissioner of Ontario —*Transparency, Privacy and the Internet: Municipal Balancing Act* , to assist municipalities in balancing the need to protect the privacy of their community members and the need to meet their other legislated obligations.
- Privacy Commissioner of British Columbia — *IT Security and Employee Privacy: Tips and Guidance* , to provide guidance for employers considering implementing IT security tools that collect employee personal information.

Internet Defamation

Defamatory Newspaper Articles and Reader Comments

Weaver v. Corcoran, 2015 BCSC 165, involved a dispute over a series of *National Post* articles (published in print and online) about global warming. The plaintiff, a climate change expert, claimed that the articles contained blatantly false and defamatory statements about him. The plaintiff sued the National Post and four journalists for defamation based on the articles (as originally published and as extensively republished on other websites and by email) and related comments posted by readers to the National Post website. The defendants vigorously defended against the plaintiff's claims.

The court held that the four articles defamed the plaintiff because an ordinary person reading the articles would infer that the plaintiff had been deceitful and was incompetent, inept, and unethical. The court rejected the defendants' various defences, and held the defendants were careless or indifferent to the accuracy of the facts in the articles but did not act with malice. The court accepted the plaintiff's argument that the defendants were liable for the extensive distribution and republication of the articles over the Internet, based on the established legal principle that an original publisher of a defamatory statement is jointly and severally liable for a republication of the statement that is authorized by the original publisher or is the natural and probable result of the original publication, and noted that the National Post website invited readers to email, tweet, or send the articles to friends.

The court rejected the plaintiff's argument that the National Post was liable for defamatory comments that had been posted to the reader comment area on the National Post website, on the basis that the National Post was not a publisher of the reader comments because the National Post was not aware of the defamatory content of the comments when the comments were posted to the website and played a passive instrumental role in their publication. The court indicated that the National Post would have been considered a publisher of the defamatory comments if the National Post had not removed the comments immediately after becoming aware of them, whether by internal review or a specific complaint brought to the attention of the National Post or its columnists. The court held that the National Post had acted promptly and did all that it could realistically do in the circumstances by removing the defamatory comments within one or two days after becoming aware of them.

The court noted that it is still early days in assessing the impact of the Internet on defamation jurisprudence, that "there is likely room for a nuanced approach when considering the emerging issues", and that as technology progresses the answer to the issue of website operator liability for defamatory reader postings might be different. The court awarded the plaintiff $50,000 in general damages and ordered the defendants to remove the offending articles from the defendants' electronic databases and Internet sites, to expressly withdraw consent previously given to third parties to re-publish the articles and to require third parties to cease republication, and to publish a complete retraction of the defamatory statements in form and content agreed to by the plaintiff or directed by the court.

Injunction against Publication and Search Site Liability

Niemela v. Malamas, 2015 BCSC 1024, involved a dispute over clearly defamatory website postings about the plaintiff lawyer and Internet search results that provided links to, and snippets of, the defamatory postings. The defamatory postings were made in 2012 and no further postings were made after police intervention, but the postings continued to be archived and accessible through Internet search sites. Approximately two years later, the plaintiff commenced two separate lawsuits — one lawsuit against the individuals responsible for the defamatory postings and another lawsuit against Google for publishing links to, and snippets of, the defamatory postings in Google search results. Google voluntarily agreed to remove the defamatory postings from Google's Canadian search site, but not from Google's other search sites. The plaintiff applied for an interlocutory injunction to compel Google to block the defamatory postings on all of its websites. Google applied for summary judgment dismissing the plaintiff's claims.

The court dismissed the plaintiff's injunction application on the basis that it was not just and equitable to grant the injunction in light of Google's voluntary agreement to remove the defamatory postings from Google's Canadian search site. The court reasoned that there was insufficient evidence of irreparable harm to the plaintiff if the injunction were not granted, because the plaintiff had not established harm resulting from searches on Google's non-Canadian search sites; the removed postings had not been replaced with new, high-ranking postings; there was no urgency, particularly in light of the plaintiff's delay in applying for the injunction; and United States statutes prohibited Google from complying with a foreign court order to block defamatory search results in the United States.

The court granted Google's application to dismiss the plaintiff's lawsuit on the basis that the lawsuit did not disclose a reasonable cause of action. The court reasoned that the plaintiff's claim for breach of privacy under the *Privacy Act* was not supported by a reasonable expectation of privacy. The court followed the Supreme Court of Canada decision in *Crookes v. Newton*, 2011 SCC 47, and held that Google was not liable for defamation by reason of Google's search engine publication of links (URLs) to defamatory postings. The court held that Google was not liable for defamation or injurious falsehood by reason of Google's inclusion of snippets of the defamatory postings because Google was not aware of the content of the snippets and was therefore acting as a mere "passive instrument" facilitator rather than as a publisher of the snippets. The court expressly noted that it was not required to consider whether Google could be liable as a publisher of the snippets and search results after Google had notice of the defamatory postings.

Liability of Blog Operators for Defamatory Posting

Baglow v. Smith, 2015 ONSC 1175, involved an acrimonious dispute between political bloggers in which one of the defendants posted to a popular political message board a statement that the plaintiff was "one of the Taliban's more vocal supporters". The plaintiff demanded the defendant message board operators immediately take down the impugned statement, but they refused to do so. The plaintiff then sued the individual who posted the impugned statement as well as the message board operators. With respect to whether the impugned statement was defamatory, the court held that the context in which the statement was published — a rough and tumble political discourse on weblogs and message boards in which participants engage in strong commentary — did not change the applicable legal test or diminish the defamatory sting of the statement. With respect to the liability of the message board operators, the court rejected the defendants' argument that a message board and its operators should not be liable as publishers for content posted by message board users. The court held that the message board operators were liable as publishers of the defamatory statement because they established the message board for the very purpose of publishing content to its readers, and they were not mere passive bystanders because they acted as moderators and administrators of the message board, made posts themselves and had the ability to control content on the message board. The court held the defendants had established a defence of fair comment, and dismissed the action.

Jurisdiction over Defamatory Online Newspaper

Goldhar v. Haaretz.com, 2015 ONSC 1128, involved a dispute over alleged defamatory statements about the plaintiff, a Toronto billionaire who owns an Israeli soccer club, published in the English online version of an Israeli newspaper. The statements, critical of the plaintiff's management of the soccer club, were read by at least several people in Ontario and over 200 people in Canada. The plaintiff sued the newspaper and the responsible reporter and editor for harm to the plaintiff's reputation in Canada. The defendants applied for an order staying the action on the basis that the court lacked jurisdiction or was not the convenient forum for the action and the action was an abuse of process. The court dismissed the application. The court held that Ontario courts had jurisdiction to hear the action because the defamation tort was committed in Ontario and the defendants had not rebutted the presumption that the alleged defamatory statements harmed the plaintiff's reputation in Ontario. The court refused to decline jurisdiction on the basis that, in light of the relevant factors (comparative convenience and expense for the parties and witnesses, applicable law, loss of legitimate juridical advantage and fairness) including the plaintiff's limitation of his claim to reputational harm suffered in Canada and the importance of permitting the plaintiff to sue for defamation where he enjoys reputation, an Israeli court was not a clearly more appropriate forum than an Ontario court. The court held that the action was not an abuse of process because the alleged defamatory statements had received more than a "minimal publication" in Ontario, and observed that it was not surprising that the plaintiff had sought to vindicate his reputation in an Ontario court.

Regulatory Matters

Canada's Anti-Spam Law ("CASL")

Computer Program Rules

The provisions of CASL regulating the commercial installation and use of computer programs on another person's computer system came into force on January 15, 2015. The sections provide that, subject to important but limited exceptions, a person must not, in the course of a commercial activity, either install or cause to be installed a computer program on another person's computer system, or cause an electronic message to be sent from another person's computer system on which the person installed, or caused to be installed, a computer program, unless the person has obtained the express consent of the owner or an authorized user of the computer system. The sections also prohibit aiding, inducing, procuring, or causing to be procured a violation of the rules regarding the installation and use of computer programs. The computer program rules apply to almost any computer program (not just malware, spyware, or harmful programs) installed on almost any computing device (including mobile phones) as part of a commercial activity (regardless of expectation of profit).

Regulatory Guidance

The Canadian Radio-television and Telecommunications Commission and the Privacy Commissioner of Canada published the following guidance documents:

- *Canada's Anti-Spam Legislation Requirements for Installing Computer Programs*, to explain CASL's rules for the installation of computer programs and CRTC's views regarding an important exception for "self-installed software".
- *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, to explain CASL's rules for consent and provide helpful guidance for CASL compliance.
- *Anti-spam law's changes to Canadian federal privacy law: A guide for businesses doing e-marketing*, to explain Canadian privacy law requirements for the use of personal information (including email addresses) to send commercial electronic messages.

Enforcement Action

The Canadian Radio-television and Telecommunications Commission and the Competition Bureau announced the following CASL enforcement action in 2015:

- *CEMs Sent without Consent or Unsubscribe Mechanism:* CRTC issued the first Notice of Violation under CASL to Compu-Finder. The Notice imposed a $1.1 million administrative penalty for "flagrantly" violating CASL by sending commercial electronic messages ("CEMs") without the recipients' consent and with an ineffective unsubscribe mechanism.
- *CEMs with Deficient Unsubscribe Mechanism:* The online dating service PlentyofFish Media entered into an undertaking (settlement), including payment of a $48,000 administrative monetary penalty, with CRTC for the alleged sending of CEMs with an unsubscribe mechanism that was not clearly and prominently set out and could not be readily performed.
- *CEMs Sent without Consent or Required Content:* The regional airline Porter Airlines entered into an undertaking (settlement), including payment of a $150,000 administrative monetary penalty, with CRTC for the alleged sending of CEMs without proof of consent and the alleged sending of CEMs that did not contain required information or have a required unsubscribe mechanism.
- *CEMs with Deficient Unsubscribe Mechanism and without Required Content:* The national media company Rogers Media Inc. entered into an undertaking (settlement), including payment of a $200,000 administrative monetary penalty, with CRTC for the alleged sending of CEMs with an unsubscribe mechanism that did not function properly or could not be readily performed or with required content that was not valid for the required minimum 60 days. In addition, Rogers Media allegedly failed to honour some unsubscribe requests within 10 business days.
- *Misleading CEMs:* The Competition Bureau commenced proceedings against two car rental companies, Aviscar and Budgetcar, seeking remedies (including $30 million in administrative monetary penalties and refunds to consumers) for alleged deceptive marketing practices (including sending false or misleading emails) regarding vehicle rental prices.
- *Malware:* The CRTC announced its first ever CASL warrant to take down a Win32/Dorkbot command-and-control server located in Toronto, Canada as part of a coordinated international effort.

Misleading Ratings of Mobile Apps

The Commissioner of Competition and Bell Canada entered into a consent agreement, filed October 14, 2015, in connection with Bell employees posting on app stores misleading, positive consumer reviews and ratings of Bell's mobile apps without disclosing that they worked for Bell (a practice known as "astroturfing"). The Competition Bureau concluded that the reviews and ratings created a "materially false or misleading general impression that they were made by independent and impartial consumers" and temporarily affected the overall rating for the apps, all in violation of *Competition Act* s. 74.01. As soon as Bell's senior management learned of the conduct, Bell removed the reviews and ratings and provided full, timely and ongoing co-operation with the Bureau's investigation. Bell agreed to not direct, encourage, or incentivize its personnel to rate, rank, or review Bell's apps in an app store, to enhance and maintain Bell's compliance program and to pay a $1.25 million administrative monetary penalty.

Miscellaneous

Injunction Prohibiting Internet Search Results

Equustek Solutions Inc. v. Jack, 2015 BCCA 265, affirming 2014 BCSC 1063, involved an application for an interlocutory injunction prohibiting Google Inc. and Google Canada (collectively "Google") from including the defendants' websites in search results generated by Google's worldwide search engines. The defendants used their websites to advertise and sell a product designed using the plaintiffs' trade secrets. The defendants ignored a court order prohibiting them from carrying on business through any website. Google, which was not a party to the lawsuit, voluntarily agreed to block some but not all of the defendants' websites from Google search results. The plaintiffs applied for an interlocutory injunction against Google on the basis that Google's search sites facilitated the defendants' ongoing breach of court orders. Google argued that the court did not have jurisdiction over Google or should decline jurisdiction, and in any event should not issue the requested injunction.

The chambers judge held that the court had jurisdiction over Google because Google, through its search sites and advertising business, carried on business in British Columbia. The chambers judge refused to decline jurisdiction over Google because Google failed to establish that another jurisdiction (California) was a more appropriate forum and the court could effectively enforce its order against Google outside Canada. The chambers judge held that the court had authority to grant an injunction with extra-territorial effect against a non-party resident in a foreign jurisdiction if it was just or convenient to do so. The chambers judge granted an injunction requiring Google to block the defendants' websites (identified in the court order) from Google's search sites worldwide. Google appealed.

The court of appeal dismissed the appeal on the basis that the injunction was within the competence of the chambers judge, did not violate any applicable legal principles or norms of freedom of speech, and was justified in the circumstances. The court of appeal held that the court had *in personam* jurisdiction over Google, even though Google did not have servers, offices, or staff in British Columbia, because a key part of Google's business involved the collection of data that resided in British Columbia or was the property of individuals in British Columbia. The court of appeal held that the granting of an injunction against third parties as an ancillary means of preserving litigating parties' rights was a well-established jurisdiction of the courts and the court had jurisdiction to make *in personam* orders with effects outside the province, but issues of comity and enforceability were concerns that must be taken into account and an order with extraterritorial effect should not be made if there were a realistic possibility that the order would offend another state's core values.

Cybersecurity — Regulatory Guidance

The Investment Industry Regulatory Organization of Canada (IIROC) published *Cybersecurity Best Practices Guide* and *Cyber Incident Management Planning Guide* to help investment dealer firms manage cybersecurity risks and prepare cyber-incident response plans. The guidance provides helpful summaries of industry standards and best practices and useful checklists. The guidance emphasizes the need for organizations to proactively manage cyber-risks and to prepare for cybersecurity incidents.

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.

[1] Copyright © 2016 Bradley Freedman and Borden Ladner Gervais LLP. All rights reserved. This paper is an abridged version of a chapter in *Annual Review of Law & Practice*, 2016, Continuing Legal Education Society of British Columbia.

By: Bradley Freedman

Services: Cybersecurity, Privacy & Data Protection, Privacy & Security Breaches, Trademarks, Technology

---