Internet and E-Commerce Law in Canada

Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law

VOLUME 14, NUMBER 11 Cited as (2013-14) 14 I.E.C.L.C. MARCH 2014

• D'OH!—FOX TEACHES INFRINGER A COSTLY LESSON •

Joanna Vatavu
McMillan LLP

In a big victory for copyright owners, particularly in the film industry, in December 2013, Twentieth Century Fox Film Corporation achieved a $10.5 million victory against the former operator of two Internet websites dedicated to streaming episodes of *The Simpsons* and *The Family Guy* television shows. In *Twentieth Century Fox Film Corporation v. Hernandez* [*Twentieth Century Fox*],[1] it was alleged that the defendant, Mr. Hernandez, had illegally copied over 700 episodes of the programs from television broadcasts and uploaded them to two websites, Watch The Simpsons Online and Watch Family Guy Online, where the episodes were made available to the public for viewing.

This case is a perfect illustration that statutory damages can be a powerful tool for copyright owners in Canada. Proving actual damages in a copyright infringement case can be difficult, particularly where the defendant is uncooperative and claims not to have any sales records. Section 38.1 of the Canadian *Copyright Act*[2] provides that copyright owners may elect to recover statutory damages instead of lost profits and damages suffered as a result of activities of infringers. Where the infringements are carried out for a commercial purpose, the Act provides for a maximum award of $20,000 in respect of all infringements relating to each individual work involved in the proceedings. In this case, the maximum statutory damages would have been more than $14 million. It was alleged that the defendant website operator profited from sales of advertising and promotional items related to the two television shows, and given the extensive number of episodes uploaded and shared by him, the court awarded $10 million in statutory damages, or approximately $14,200 per infringing work.

• In This Issue •

LexisNexis

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ontario L3T 7W8

ISBN: 0-433-42472-9 **ISSN 1494-4146**
ISBN: 0-433-44385-5 (print & PDF)
ISBN: 0-433-44674-9 (PDF)

Subscription rates: $230 per year (print or PDF)
$335 per year (print & PDF)

Please address all editorial inquiries to:

Boris Roginsky, Journals Editor
LexisNexis Canada Inc.
Tel. (905) 479-2665; Toll-Free Tel. 1-800-668-6481
Fax (905) 479-2826; Toll-Free Fax 1-800-461-3275
Internet e-mail: ieclc@lexisnexis.ca.

The balancing act involved in arriving at the appropriate figure to be awarded for each infringed work has received some attention from the courts in recent years, with a continuing trend in awarding significant statutory damages against copyright infringers, including website operators who illegally upload and share copyrighted works. In exercising their discretion, courts must take into account all relevant factors, including the factors set out in subs. 38.1(5) of the *Copyright Act*—namely, the good faith or bad faith of the defendant, the conduct of the parties before and during the proceedings, and the need to deter other infringements of the copyright in question. This suggests that the list is not exhaustive and other factors may be taken into account in each particular case.

Another decision of the Federal Court giving a similarly high award of statutory damages in the copyright context is *Entral Group International Inc. v. Mcue Enterprise Corp*.[3] There, the defendants acquired copies of the plaintiffs' copyrighted songs and reproduced them by installing copies onto karaoke machines that enabled customers to publicly perform the works in exchange for a fee. The court found that the unauthorized presentation of a work in a commercial establishment was an infringement of the copyright holder's right to perform the work in public and had no difficulty in concluding that the defendants had economically benefited from the infringement of the plaintiffs' copyright interests. The court awarded statutory damages in the amount of $15,000 per infringed work in respect of each of the seven titles that were the subject matter of the proceeding. Among the factors considered by the court in reaching its decision on the quantum of statutory damages were (1) the willful and ongoing infringement that continued over seven years; (2) the multiple occasions on which the plaintiffs had notified the defendants of their infringing activities; (3) the

plaintiffs' reasonable conduct in offering the defendants a typical licence agreement for the use of their copyrighted works; and (4) the defendants' deplorable conduct in choosing to stonewall the plaintiffs, resist the licensing arrangements offered by the plaintiffs, and continue their infringing activity. The court also awarded punitive and exemplary damages of $100,000 and solicitor-client costs for the defendant's reprehensible conduct.

The United States *Copyright Act* also contains provisions for awards of statutory damages in lieu of actual damages, which range from $750 to $30,000 in respect of any one copyrighted work "as the court considers just", regardless of whether the infringing activity was committed for a commercial or non-commercial purpose.[4] This sum may be increased up to $150,000 per individual work where it can be shown that the infringement was committed willfully.

Although statutory damages for copyright infringement can be an appealing remedy to content owners, especially where damages are difficult to quantify or where actual damages are not significant, the statutory damages calculation can, at times, lead to absurd results, particularly in cases of mass infringement found in the context of online peer-to-peer file sharing. In a recent decision by the United States District Court for the Southern District of New York,[5] the court found that the plaintiffs' suggested award for statutory damages was absurdly large. The plaintiffs identified approximately 11,000 sound recordings that they alleged had been infringed through the LimeWire system, a peer-to-peer sharing network. If one were to calculate the statutory damages award at the maximum allowable amount of $150,000 for each individual work, it meant the defendants faced a potential award of over a billion dollars in statutory damages. The court went on to state that if the plaintiffs were able to pursue a statutory damage theory predicated on the number of direct infringers per work, which the plaintiffs advanced, the damages could reach into the trillions. The court rejected the plaintiffs' statutory interpretation as it would award them "more money than the entire music recording industry has made since Edison's invention of the phonograph in 1877", which it found to be an absurd result.

Nevertheless, the threat of a statutory damages award can be a strong enough deterrent for potential infringers by preventing their unjust enrichment in instances where either the infringer is uncooperative and damages would be difficult to prove or actual damages would not be significant.

While statutory damages can be a powerful remedy for copyright owners, the *Copyright Act* also has another significant remedy that is worth considering. Generally, a plaintiff can obtain only an injunction prohibiting the defendant from repeating the infringements specifically addressed in the lawsuit. However, s. 39.1 of the *Copyright Act* permits the court to grant a "wide injunction" restraining infringement of not only the works in issue but any other works owned by the plaintiff. In the *Twentieth Century Fox* case, the Federal Court granted a wide injunction against the defendant, prohibiting him from any further infringing dealings with not only the works involved in the proceedings but also any other works in which Twentieth Century Fox Film Corporation owns copyright, including works that come into existence after the date of the judgment.

The court in *Twentieth Century Fox* also found that the defendant's repeated, blatant, and intentional misconduct merited an award of punitive damages to serve as deterrence and punishment for such illegal activities. The court ordered an award of $500,000 in this respect.

The *Twentieth Century Fox* case is one of the larger statutory damage awards a copyright owner has obtained in Canada. The wide injunction granted by the court also serves to significantly impair the defendants' future business prospects. In its decision, the Federal Court strongly condemns Internet piracy and sends a message to those who build businesses around illegal file sharing in Canada that it is prepared to use all the tools in the *Copyright Act* to stamp it out.

[*Editor's note*: **Joanna Vatavu** is a member of the Technology and IP Group at McMillan LLP where she practises in all areas of intellectual property with an emphasis on copyright and trade-mark matters. Joanna received her J.D. in 2010 from Osgoode Hall Law School.

[1] *Twentieth Century Fox Film Corporation v. Hernandez*, Court File No. T-1618-13, Federal Court (December 3, 2013).
[2] R.S.C. 1985, c. C-42.
[3] [2010] F.C.J. No. 723, 2010 FC 606.
[4] United States *Copyright Act*, 17 U.S.C. §504(c).
[5] *Arista Records LLC v. Lime Group LLC* (2011) 784 F. Supp. 2d 313.

• CAN YOU CARRY OUT BITCOINS ACTIVITIES IN CANADA WITHOUT LEGAL RISKS? •

Nathalie Beauregard, *Partner*
Osler, Hoskin & Harcourt LLP

Bitcoins are a digital currency and have become widespread on the Internet, and some companies have begun to accept these items as payment for real goods and services. This virtual currency has been subject to media scrutiny of late due to certain problems experienced by industry players.[1]

At the time of writing, Bitcoins are not explicitly and specifically governed by any laws or litigation. However, on February 11, 2014, as part of the federal budget, James Flaherty, finance minister of Canada, proposed regulation of virtual currencies, including Bitcoins. Such currencies are described within the budget as potential threats to the fight against money laundering and financing of terrorism. In order to keep pace with these emerging threats, the government plans to act via legislative amendments in order to regulate virtual currencies. Though it is clear that the government intends to subject those currencies to regulation, there are few details given regarding the planned amendments.

To implement the proposed regulation of currencies like Bitcoins, the federal budget suggests allocating $10.5 million over five years and as much as $2.2 million per year ongoing to the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). Furthermore, the government proposed providing an additional $12 million on a cash basis over five years to improve FINTRAC's analytics system.

While there are plans to regulate Bitcoins, there is still no certainty at this stage. It is likely that the sale (or exchange) of Bitcoins will fall under the scope of "Money Services Businesses", given that the term *currency* is used to describe Bitcoins in the federal budget.

If Bitcoins are, in fact, qualified as money or currency, this will trigger the application of the laws regulating money services businesses, including anti–money laundering laws and rules governing foreign exchange. Regulators in charge of implementing those laws, especially securities regulators and FINTRAC, have significant powers

that allow them to interpret broadly to include Bitcoins in their fields of application.

Under federal legislation, money services businesses must register with FINTRAC. In addition, they have several obligations such as (1) taking specific measures to ascertain the identity of individuals and entities with which they are dealing as well as (2) reporting and record keeping requirements. In addition, if the money services businesses are subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*,[2] they must report

- suspicious transactions;
- possession or control of property that is owned or controlled by or on behalf of a terrorist or terrorist group;
- large cash transactions involving amounts of $10,000 or more received in cash; and
- international electronic funds transfers of $10,000 or more, including the transmission of instructions for a transfer of funds made at the request of a client through any electronic, magnetic, or optical device, telephone instrument, or computer.

In Quebec, money services businesses are subject to several obligations such as

- holding a licence;
- paying annual fees;
- being of good moral character;
- verifying the identity of its customers;
- maintaining records and registers; and
- filing of prescribed reports, documents, and statements.

In addition, although not obviously, Bitcoins could be considered a "security" or a "derivative" under applicable securities legislation. As a consequence of that interpretation, in order to move forward with the Bitcoins activities, you would have to comply with all obligations of securities issuers or distributors, which may entail dealer registration, prospectus delivery, and other requirements unless exceptions are available.

Finally, if you perform Bitcoins activities, you may also have to comply with consumer protection legislation in each of the provinces in which your clients are located. For instance, the *Consumer Protection Act* (Quebec) [*CPA*][3] governs all contracts entered into with consumers via the Internet (*i.e.*, without being in the consumer's presence). The *CPA* provides that a merchant must disclose specific information in a certain format before entering into such a contract.

Given the high degree of uncertainty in Canada with respect to carrying out Bitcoins activities and given the resulting high degree of legal risks associated with Bitcoins, in our view, the most appropriate way to mitigate these risks is to consult with the relevant regulators in order to obtain prior approval or guidelines before carrying out Bitcoins activities.

[*Editor's note*: **Nathalie Beauregard** practises business law and has significant experience in technology matters. She acts for a broad spectrum of companies including businesses established to commercialize newly acquired technologies. She is a member of the Quebec and New York Bars. She may be reached at 514-904-8121.]

---

[1] On February 28, 2014, the Mt. Gox Bitcoin exchange filed for bankruptcy protection after 850,000 Bitcoins, valued at nearly half a billion dollars, disappeared. A press release issued by the company on that same date announced that the application made by the company for commencement of a procedure of civil rehabilitation had been accepted. The company stated in the press release that "illegal access through

the abuse of a bug in the Bitcoins system resulted in an increase in incomplete Bitcoins transfer transactions". This bug, known as "transaction malleability", has also been blamed for the attack on Silk Road 2.0 where the reserve of Bitcoins disappeared under similar circumstances. While a definitive reason for the missing Bitcoins remains unknown, the situation highlights the concerns surrounding regulation, or lack thereof, of Bitcoins and other digital currencies.

[2] SOR /2002-184.

[3] CQLR c P-40.1.

• IS USING HEALTH INFORMATION FOR INTEREST-BASED ADVERTISING REALLY OFF LIMITS? •

Timothy M. Banks, Partner
Dentons Canada LLP

As was widely reported, on January 15, 2013, the Office of the Privacy Commissioner of Canada ("OPC") issued a Report of Findings regarding interest-based advertising, or online behavioural advertising, through Google's AdSense service.[1]

Discussions of the case frequently suggested that Canadian law does not permit the use of "health information" for interest-based advertisements. This is debatable, but, in any event, this seems to miss what the case was really about. The issue appears to have been whether Google exercised sufficient due diligence in monitoring its customers' compliance with its terms. This makes for less catchy a headline but may have more significant implications in the long run.

What the Complaint Was about

According to the Report of Findings, the complainant searched for a particular type of medical device for sleep apnea. Importantly, the complainant was signed in to his Google account when he made those searches. Subsequently, the complainant began to see targeted advertising (relating to his searches) on other sites.

Google participates in the AdChoices program, and advertisements often include the AdChoices icon indicating that their page involves interest-based advertising or online behavioural advertising ("OBA"). By clicking on the icon, users can opt out of interest-based advertising.

Although the complainant browsed while signed in to this Google account (and appears not to have opted out), the complainant argued, according to the Report of Findings, that "he did not provide Google with consent to display his personal medical information in browsers".[2]

Contextual Advertisements versus OBA

Previously, the OPC has distinguished contextual advertising (based on the content of a page) from interest-based, a.k.a. online behavioural, advertising (based on "tracking" user interests across websites).[3]

Initially, Google disputed that the advertising was OBA and claimed that it was based on recent or related page content that, according to the Report of Findings, "appeared out of context to the user".[4] However, subsequently, Google appears to have conceded that the advertising was placed as a result of a Google customer's AdWords remarketing program.[5]

The AdWords remarketing program allows Google customers to install a code provided by Goggle on their websites. This code installs a cookie ID in the user's web browser unless the user has opted-out of interest-based advertising or OBA. The Google customer can then design

an advertising campaign (that the user will see on other web pages) that uses Google's advertising products. This is interest-based advertising or OBA.

Google's Policy

The problem for Google was that its privacy policy stated it did not use any collected information for advertising based on health:

> [w]e use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services […] When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.[6]

Although Google requires advertisers to agree to specific policies that prohibit OBA based on "health or medical information", the customers could use the products in violation of these policies because the customer is in control.

According to the OPC, Google's practice did not correspond to the actual wording of the privacy policy as outlined above.[7] Moreover, the OPC was of the view that meaningful consent was required. Implied or "opt-out" consent was only permissible for "non-sensitive" information. Health information was "sensitive".[8]

But Is Health Information Really Off Limits?

The OPC (perhaps incorrectly) equated implied consent with "opt-out" consent. Leaving aside that debate, it appears that the OPC is reinforcing previous guidance that express consent should be used when conducting interest-based advertising using sensitive information.

Principle 4.3.6 of the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*] states:

> The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).[9]

Importantly, however, subs. 5(2) of *PIPEDA* states that "[t]he word "should" […] indicates a recommendation and does not impose an obligation". Whether a court would agree that express consent is always required even if the Ad Choices program is prominently used (and the website Privacy Notice is clear) is open for debate.

What Does the Future Hold in This Case

What is not open for debate is that Google's privacy policy said that it was not using health information for advertising purposes. Although its customers were doing so in violation of this policy, the OPC concluded that Google did not have a sufficiently rigorous and scalable compliance program to ensure enforcement.[10] Google was, in effect, required to be a gatekeeper.

To remedy this situation, Google undertook initiatives

- to reject remarketing campaigns involving the sleep apnea treatment devices,
- to clarify its policies to advertisers,
- to develop new training for internal teams,
- to increase monitoring of advertiser's remarketing campaigns,
- to upgrade automated screening systems.

Bottom Line

The bottom line is that the practice of Google's customers did not comply with Google's policies and the OPC was not satisfied with Google's due diligence in enforcing its policies.

Whether health information is always off limits to interest-based advertising is not at all clear. On the one hand, the OPC suggests it is absent express consent; however, whether this view will ultimately prevail on the current wording of *PIPEDA* is uncertain, particularly if an organization prominently draws its practices to the attention of the consumer and provides an immediate opt-out mechanism. On the other hand, this may be one of those uses of personal information that simply fails the test of reasonableness under subs. 5(3) of *PIPEDA*.

[*Editor's note*: **Tim Banks** advises on data governance and consumer protection laws and regulations. He is the Canadian Lead for Dentons' Global Privacy and Data Security practice. He is also a Partner in the Business Law Department where he provides advice with respect to Consumer Protection laws and regulatory issues relating to Marketing and Advertising.]

---

1 Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2014-001* (January 2014), <https://www.priv.gc.ca/cf-dc/2014/2014_001_0114_e.asp> ("Report of Findings").

2 *Ibid*., para. 7.

3 Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising* (June 2012), <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.

4 *Supra* note 1, para. 18.

5 *Ibid*., para. 33.

6 *Ibid*., para. 25.

7 *Ibid*., para. 26.

8 *Ibid*., para. 27.

9 S.C. 2000, c. 5, Schedule 1.

10 *Supra* note 1, para. 45.