Federal Court  Cour fédérale

**Date: 20220606**

**Docket: T-513-18**

**Citation: 2022 FC 827**

**Toronto, Ontario, June 6, 2022**

**PRESENT: The Honourable Madam Justice Furlanetto**

***SIMPLIFIED ACTION***

**BETWEEN:**

**VOLTAGE HOLDINGS, LLC**

**Plaintiff**

**and**

**DOE#1 *ET AL* (SEE SCHEDULE 1 FOR LIST OF DEFENDANTS)**

**Defendants**

**and**

**SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC**

**Intervener**

**ORDER AND REASONS**

[1] This is a motion for default judgment brought pursuant to Rule 210 of the *Federal Courts Rules*, SOR/98-106 [Rules] relating to an action under the Federal Court's simplified procedure for online copyright infringement. The Plaintiff, Voltage Holdings, LLC [Voltage], a movie production company, alleges that a mass group of internet subscribers used or authorized for use the BitTorrent peer-to-peer [P2P] network to unlawfully make the Plaintiff's science-fiction film, *Revolt* [the Work] available for distribution. The Plaintiff seeks default judgment against thirty internet subscribers [Default Defendants] as well as statutory damages and costs from each. A list of the Default Defendants, identified by IP address, is attached as Schedule "A".

[2] Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic [CIPPIC], a legal clinic based at the University of Ottawa and public interest intervener, was previously granted leave to intervene in the motion. It provided written submissions and argument at the hearing.

[3] For the reasons that follow, I find that there is insufficient evidence to grant default judgment, but that Rule 210(4)(c) should be exercised and the matter should proceed forward to trial, without prejudice to the Plaintiff to bring the same motion back again with better evidence.

## I. Background

[4] The Plaintiff is a motion picture production company. It hired a service company Maverickeye UG [Maverickeye] to use forensic data collection software [Software] to monitor the internet to look for unauthorized uploading and offering of its movies, including the Work, through the BitTorrent network.

[5] As explained by the Plaintiff's affiant, Benjamin Perino, BitTorrent is a protocol that allows for the transfer of large files between internet users on a P2P network. Rather than downloading a file from a single source server, the BitTorrent protocol allows users to join a "swarm" of hosts and upload and download files simultaneously in a decentralized manner. In P2P sharing, a computer program that implements the BitTorrent protocol requests a file and portions of the requested file residing on other devices connected to the P2P network are then sent and reassembled into a full copy on the end user's device. Users do not typically copy an entire file from one peer, but rather from multiple peers that have already downloaded the file and have made it available through their BitTorrent software. Typically, when users copy a file they simultaneously offer to distribute portions of it to every other user connected to the BitTorrent network. The goal of the system is to distribute files over many computers and internet connections, which in turn tends to minimize data transfer from any one individual (Paragraphs 5-13, Affidavit of Benjamin Perino, affirmed May 28, 2021 [Perino Affidavit]).

[6] The Software tracks people offering files for download and requests portions of a file from a user who has made the file available. After confirmation that the downloaded portion matches the relevant work, the Software captures certain information about the file, including the Internet Protocol [IP] address of the user, the date and time the file was made available, the metadata of the file identifying the name and size of the file, and a "hash" signature identifying the version of the work.

[7] In 2017, the Software detected and verified portions of the Work being made available for download through the BitTorrent network from various IP addresses. Based on this

information, the Plaintiff sent notices to the related internet service providers [ISPs] to forward to the relevant internet subscribers associated with the IP addresses pursuant to the notice-and-notice regime set out by sections 41.25 and 41.26 of the *Copyright Act*, RSC, 1985 c C-42 [Act].

[8] The first notice gave the internet subscriber one week to remove the copy of the Work from the computer using the internet account or to be subject to the possibility of an action for copyright infringement. A second similar notice was sent where the Software located the same IP address offering the same Work after the seven day period set out in the first notice. The ISPs confirmed the notices were sent to the relevant internet subscribers.

[9] This action was commenced on March 16, 2018. In the Statement of Claim [SOC], the predecessor to the Plaintiff named 110 anonymous "Doe" Defendants, identified only by their IP addresses as determined by the Software.

[10] On December 3, 2018, the Plaintiff's predecessor obtained a *Norwich* order requiring the relevant ISPs to disclose the names and addresses of the subscribers of the IP addresses listed in the SOC.

[11] The Plaintiff seeks relief against thirty internet subscribers that it describes as the "worst of the worst". The Plaintiff asserts that the thirty Default Defendants are the internet subscribers associated with those IP addresses that offered the Work for download online "for weeks, sometimes months, possibly to thousands of people." The degree of alleged infringement was assessed by considering the length of time within a three month period before and after the

notices that portions of the Work were made available for download and by considering the swarm size of the offering.

[12] In support of its motion, the Plaintiff filed two affidavits: (1) the Perino Affidavit; and (2) an Affidavit of Marnie Macdonald, affirmed May 31, 2021 [Macdonald Affidavit].

[13] Mr. Perino is the former Chief Executive Officer and a Senior Developer at GuardaLey Ltd, a company created to monitor the download and distribution of copyrighted works. Mr. Perino developed the Software which was licensed to Maverickeye and used to track and identify the IP addresses distributing the Work via the BitTorrent network.

[14] Ms. Macdonald is a law clerk working for the solicitors for the Plaintiff. Ms. Macdonald provides background to the proceeding, the investigations conducted using the Software, the notices delivered, service of the SOC, and the infringement analysis conducted.

[15] As no defences were filed in the action, the evidence in the Perino and Macdonald Affidavits is uncontested.

[16] As noted earlier, CIPPIC was granted leave to intervene in the motion. It filed written submissions and gave oral argument at the hearing.

## II. The Issues

[17] This motion raises the following issues:

1. Was service of the SOC sufficient to establish that the Default Defendants are in default?

2. Should default judgment be granted: Does the evidence establish that the Default Defendants, who are internet subscribers, have infringed copyright in the Work?

3. If so, what quantum of statutory damages is the Plaintiff entitled to?

## III. Analysis

### A. *Was service of the SOC sufficient to establish that the Default Defendants are in default?*

[18] On September 24, 2018, Prothonotary Milczynski, the Case Management Judge, ordered that service of the SOC by registered mail to the Defendants' addresses disclosed pursuant to any Order of the Court for disclosure would be deemed personal service under Rule 128(1)(b) of the Rules if the Defendant or an adult member of their household signed for the package. If the package was unclaimed, the Plaintiff was to effect service by mailing a copy of the SOC by regular mail. The Order also provided that no default could be commenced without personal service of the SOC being effected in accordance with Rule 128(1)(b) and proof of service filed, unless otherwise ordered by the Court.

[19] Rule 128 of the Rules provides for personal service of a SOC on an individual:

| | |
|---|---|
| […] | […] |
| (b) by leaving the document with an adult person residing at the individual's place of residence, and mailing a copy of the document to the individual at that address; | b) par remise du document à une personne majeure qui réside au domicile de la personne et par envoi par la poste d'une copie du document à cette dernière à la même adresse; |
| […] | […] |

| | |
|---|---|
| (e) by mailing the document by registered mail to the individual's last known address, if the individual signs a post office receipt; . . . | e) par envoi par courrier recommandé du document à la dernière adresse connue de la personne si la personne signe le récépissé du bureau de poste; |

[20] The Macdonald Affidavit provides details of the service made on the thirty internet subscribers who are identified by the Plaintiff as the Default Defendants. The evidence indicates that:

(a) Twenty of the Default Defendants had the individual identified by the *Norwich* order sign personally for the registered mail package that included the SOC;

(b) Eight Default Defendants had an individual other than the individual identified by the *Norwich* order sign for the registered mail package that included the SOC;

(c) The registered mail package was not successfully delivered to one Default Defendant (Doe #15), but the SOC was sent to that Defendant by regular mail; and,

(d) There was no proof of delivery of the registered mail package for one other Default Defendant (Doe # 51).

[21] Service on the first group satisfies the requirements of personal service under Rule 128(1)(e).

[22] With respect to the second group, the Plaintiff asserts that it is reasonable to assume from the circumstances of the acceptance of the registered mail package that an adult signed for the

service package and that the package was directed to the Default Defendant. In all cases, a further reminder letter was also sent to all individuals identified by the *Norwich* order that fell into this group, except for Doe #24 with whom there was correspondence between the Default Defendant and counsel for the Plaintiff. There is no indication that any of this correspondence was ever returned. On the basis of my review of the service material, I am satisfied that it is likely that the SOC came to the Default Defendants' attention and that service for this group should be validated.

[23] With respect to the remaining two Default Defendants (Doe #15 and Doe #51), the Plaintiff has included correspondence between the Default Defendant or their counsel and the Plaintiff's counsel regarding the action. I am satisfied that this correspondence indicates that Doe #15 and Doe #51 were aware, and had notice, of the action. Accordingly, I consider it appropriate to validate service on these Defendants.

[24] CIPPIC argues that the Plaintiff should not be entitled to bring a default proceeding as it hasn't done enough to identify the true Defendants who actually performed the activities asserted to be infringing. It contends that the Plaintiff should have requested discovery of the internet subscribers or requested a second *Norwich* order to identify the true users' identities. However, it is up to the Plaintiff to define who it is asserting is the infringer. In my view, CIPPIC's argument goes to the merits of the motion; that is, whether infringement has been established by the asserted defendants (the internet subscribers), rather than whether the motion can be brought. Accordingly, I will consider this argument further below in my discussion of the issue of infringement.

[25] CIPPIC further contends that the default motion should not proceed as there is improper joinder of the Default Defendants in one proceeding. I agree with the Plaintiff, as joinder is not an issue raised by the Plaintiff on this motion, it is outside the scope of the intervention order, which limited CIPPIC's intervention to only those issues that were already in dispute. Moreover, there are no distinguishing facts that have emerged at this stage to suggest that joinder is inappropriate or inefficient to address the default claim against the group of Default Defendants.

[26] As none of the Default Defendants filed a Statement of Defence within 30 days of being served with the SOC or at all, I am satisfied that the Default Defendants are indeed in default and that the Court should proceed to consider the merits of the motion and whether default judgment should issue.

B. *Should default judgment be granted: Does the evidence establish that the Default Defendants, who are internet subscribers, have infringed copyright in the Work?*

[27] In order for the Plaintiff to obtain relief for copyright infringement, it must first establish that it owns copyright in the Work.

[28] If a name purporting to be that of the maker of the work appears on the work in the usual manner, that person is presumed to be the maker of the work, and the maker is presumed to own copyright (s. 34.1(1) of the Act; *Canadian Broadcasting Corporation v Conservative Party of Canada*, 2021 FC 425 at para 33). In the end credits of the Work it includes a written inscription that the owner of the copyright is POW Nevada, LLC. The Plaintiff has provided a copy of the assignment of copyright in the Work from POW Nevada LLC to the Plaintiff. In my view, these

facts are sufficient to entitle the Plaintiff to the presumption of ownership of copyright in the Work.

[29] Direct Infringement is addressed in subsection 27(1) of the Act, which states that: "[i]t is an infringement of copyright for any person to do, without the consent of the owner of the copyright, anything that by this Act only the owner of the copyright has the right to do."

[30] Pursuant to subparagraph 3(1)(f) and subsection 2.4 (1.1) of the Act, a copyright owner has the exclusive right to communicate a work to the public by telecommunication, including in a way that allows a member of the public to have access to the work from a place and at a time individually chosen by that member of the public. A person infringes copyright if they violate these exclusive rights.

[31] In *Entertainment Software Association v Society of Composers, Authors and Music Publishers of Canada*, 2020 FCA 100 at paragraphs 55-56 (leave to appeal to the SCC granted, 39418 (22 April 2021)), the Federal Court of Appeal confirmed that paragraph 2.4 (1.1) of the Act was intended to clarify that the unauthorized sharing of copyrighted material over P2P networks constitutes an infringement of copyright.

[32] The uncontested evidence indicates that portions of the Work have been made available through the BitTorrent network, by persons who are not the owner or individuals authorized by the owner, in a manner that allows BitTorrent users to have access to the portions of the Work at a chosen place and time. Mr. Perino's evidence states that for each Default Defendant on at least

two occasions, the Software detected a person using the Default Defendant's IP address to make a portion of the Work available for download over the BitTorrent network and distributed a copy of a portion of the Work (uploaded a portion of the Work) to the Software in response to a request for download. In each case, there were two comparisons completed by employees of Maverickeye to confirm that the downloaded portion was a copy of a portion of the Work. Similarly, the Software was able to verify that in each instance, the IP address used to offer the portion of the Work for download was the same in each of the two occurrences.

[33] Thus, portions of the Work have been subject to unauthorized sharing over the BitTorrent network. The outstanding issue is whether the Default Defendants who are internet subscribers have committed an act of infringement.

[34] The Plaintiff put forward two theories of infringement in oral argument; either direct infringement or infringement by authorization.

(1) Is there Direct Infringement?

[35] The Plaintiff bears the burden of establishing infringement on a balance of probabilities through clear, convincing and cogent evidence: *FH v McDougall*, 2008 SCC 53 at paras 40, 45-46. The Plaintiff asserts that it has done all that it can to meet this burden. It contends that it has identified the internet subscribers responsible for the thirty IP addresses at issue and sent two notices to each (under the notice and notice regime) in an effort to deter infringement. It argues that as no defence has been filed, there are no additional facts in the proceeding to assist with identification of the users of the IP addresses in issue, and there is no technological way to pierce

through the veil of the internet to determine who was actually using the IP addresses at the time the Work was offered for download.

[36] CIPPIC contends that the Plaintiff has failed to identify the persons who were accessing the computers at the time the Work was being offered and who are responsible for any alleged infringement. It asserts that it cannot be presumed that an internet subscriber and an internet user are the same person.

[37] CIPPIC refers to the decision in *R v Ward*, 2012 ONCA 660 [*Ward*], where the Ontario Court of Appeal noted this gap at paragraph 23:

> The ISP records the dates and times that its IP addresses are assigned to its subscribers. These records identify the subscribers' accounts on which the Internet was accessed at particular times. However, that does not necessarily mean that the subscriber himself or herself was using the computer connected to the Internet at that time, or that it was even the subscriber's computer that was connected to the Internet. A wired or wireless network may link multiple computers to a central device referred to as a shared access point. When more than one computer is accessing the Internet through a shared access point at the same time, there are additional technical issues that may arise.

[38] The reasoning in *Ward* was similarly applied in *United States v Viscomi*, 2015 ONCA 484 [*Viscomi*], which involved consideration of an extradition order. The Court at paragraphs 31 and 35-36 found that the inference that Mr. Viscomi was the user of an IP address at the relevant time was not one that could reasonably and logically be drawn from the fact that he was the subscriber of that IP address. The gap between the subscriber information and the factual inference that Mr. Viscomi was the user of the IP address at the relevant time could only be

bridged by evidence. As such, the order committing Mr. Viscomi for extradition to the United States was quashed.

[39] Both the *Ward* and *Viscomi* decisions, however, involved criminal proceedings, which carry a distinct standard of proof and an ability on behalf of the Crown to obtain search warrants and to compel testimony and documents. I agree with the Plaintiff that the role of the internet subscriber must be considered in the appropriate context, which in this case is the notice and notice regime under the Act.

[40] The notice and notice regime was discussed in *Rogers Communications Inc v Voltage Pictures LLC*, 2018 SCC 38 [*Rogers*] at paragraphs 22-23 as serving two complementary objectives: deterring online copyright infringement; and balancing the rights of interested parties. With respect to the first objective, it was noted that "by requiring notice of a claimed infringement to be forwarded to the person who was associated with the IP address that is alleged to have infringed copyright, the regime is aimed at deterring that person, or others who are using the IP address, from continuing to infringe copyright". As described by the Supreme Court at paragraph 24:

> [24] The notice and notice regime was not, however, intended to embody a comprehensive framework by which instances of online copyright infringement could be eliminated altogether. As a representative of Rogers explained before the House of Commons committee considering what would become of the *Copyright Modernization Act*, "notice and notice is not a silver bullet; it's just the first step in a process by which rights holders can go after those they allege are infringing. ... Then the rights holder can use that when they decide to take that alleged infringer to court" (House of Commons, Legislative Committee on Bill C-32, *Evidence*, No. 19, 3rd Sess., 40th Parl., March 22, 2011, at p. 10). This is why, as I have explained, a copyright owner who wishes to sue a person

> alleged to have infringed copyright online must obtain a *Norwich* order to compel the ISP to disclose the person's identify. The statutory notice and notice regime has not displaced this requirement, but operates in tandem with it. This is affirmed by s. 41.26(1)(b), which contemplates that a copyright owner may sue a person who receives notice under the regime, and fixes the ISP's obligation to retain records which allow that person's identity to be determined for a period of time after such notice is received.

[41] With respect to balancing the rights of interested parties, the Supreme Court in *Rogers* noted at paragraphs 26 and 27:

> [26] For example, Parliament sought to strike a balance between the interests of copyright owners and of Internet subscribers, respectively, by preferring a notice and notice regime over a "notice and take down" regime (see *House of Commons Debates*, at p. 2109, per Hon. James Moore). ... the notice and notice regime allows for notices of claimed infringement to be forwarded (thereby advancing the rights of copyright holders), while accounting for the interests of Internet subscribers by maintaining the presumption of innocence and allowing them to monitor their own behaviour (and, more specifically, to avoid continued copyright infringement).
>
> [27] Parliament also sought to balance the interests of copyright owners against those of Internet intermediaries such as ISPs. ... the amendments to the Act were also intended to "clarify Internet service providers' liability" to copyright owners (*Copyright Modernization Act*, summary; see also Legislative Committee on Bill C-32, *Evidence*, at p. 1, per Craig McTaggart). To that end, Parliament insulated ISPs from liability for the copyright infringement of their Internet subscribers (Act, s. 31.1). Now, to attract liability under the Act, an ISP must fail to satisfy its statutory obligations under the notice and notice regime, or provide a service "primarily for the purpose of enabling acts of copyright infringement" (ss. 27(2.3), 31.1 and 41.26(3)).

[42] In my view, these comments, which refer back to the objectives of Parliament in implementing the notice and notice regime, highlight that litigation by rights holders against internet subscribers was contemplated if deterrence was not achieved by the notice and notice system. However, it does not suggest an absolute liability framework. As stated, there is a

presumption of innocence for internet subscribers. Infringement by internet subscribers (either directly or through authorization), in my view, must still be proven for the claim to succeed.

[43] This same theme was further emphasized at paragraph 41 of *Rogers*, wherein the Court stated:

> [41] It must be borne in mind that being associated with an IP address that is the subject of a notice under s. 41.26(1)(a) is not conclusive of guilt. As I have explained, the person to whom an IP address belonged at the time of an alleged infringement may not be the same person who has shared copyrighted content online

[44] The Plaintiff asserts that it has provided comprehensive evidence of significant and repeated infringement. It has the names and addresses of the internet subscribers that it knows are associated with the IP addresses from which it asserts there is repeated infringing use. Where the defendant has failed to engage and provide further information, the Plaintiff asserts that the persuasive (legal) burden applies, shifting the burden to the Default Defendants to disprove their association with the acts concerned at the IP addresses: Sopinka, Lederman & Bryant: The Law of Evidence in Canada, 5th ed. (Toronto: LexisNexis Canada, 2018) at §3.11-§3.15.

[45] I do not agree that the burden shifts so easily. In a default proceeding all allegations in the statement of claim are treated as denied and the plaintiff bears the burden of proof: *Tatuyou LLC v H2Ocean Inc*, 2020 FC 865 at para 9; *NuWave Industries Inc v Trennen Industries Ltd*., 2020 FC 867 at paras 16-17. The Plaintiff is required to lead sufficient evidence to allow the Court to conclude on a balance of probabilities that the Default Defendants are the proper defendants and have infringed copyright.

[46] CIPPIC contends that despite the defendants being in default, the Plaintiff should not be entitled to obtain judgment without exhausting the procedural means available to obtain further information. It asserts that the Plaintiff could have sought leave to obtain discovery of the internet subscribers under Rule 236(1)(c) of the Rules, which provides that a party may examine an adverse party for discovery if the adverse party is in default of serving and filing its pleadings and leave of the Court has been obtained. If identifying an IP address associated with allegedly infringing activity is sufficient to maintain an action for primary infringement, CIPPIC asserts it would encourage unscrupulous actors to litigate and run counter to the purposes of the Act.

[47] The Plaintiff argues that even if discovery were available, it would require the Plaintiff to obtain all electronic devices associated with the IP address, or forensic copies of the devices, of all individuals with access to the IP address on the relevant dates in order to definitively establish who was using the computer at the relevant time. The intrusion into the privacy of these individuals would be significant and the costs of the analysis high. Similarly, asking third party ISPs to provide detailed internet activity logs of their subscribers would raise significant privacy concerns or require expert assistance if in fact the evidence existed in a useful form.

[48] It notes that the Court has previously expressed reluctance in ordering disclosure of information about subscribers in order "to make sure that privacy rights are invaded in the most minimal way" (*Voltage Pictures, LLC v John Doe*, 2016 FC 881 at para 16; rev'd other grounds 2017 FCA 97; rev'd other grounds 2018 SCC 38).

[49] The Plaintiff refers to paragraph 46 of *Rogers*, which states that "the notice and notice regime should be interpreted so as "to allow copyright owners to protect and vindicate their rights as quickly, easily and efficiently as possible while ensuring fair treatment of all"". It contends that to require it to do more would place an unreasonable burden on the Plaintiff, tipping the balance in favour of the rights users and making it impossible for any reasonable enforcement of online copyright infringement.

[50] I agree with the Plaintiff that if leave for discovery were granted, the scope of allowable discovery would likely only be limited, particularly in the context of a simplified proceeding such as this. However, this does not mean that some further discovery or a request for further information would be futile. Without seizing the electronic devices at the address, written discovery could be used to seek further information as to the nature of the system provided at the IP address, including how many devices the IP address services, the type of interaction or control the IP owner has over those devices and its users, how many users there are, and what if any steps were taken with respect to those users after the notices under the notice and notice regime were received. Such information would assist with understanding the role of the internet subscriber.

[51] The Perino Affidavit states that the ISP's customer may be (and often is) the individual who is utilizing BitTorrent software to distribute files, particularly if the assigned IP address is only used by a single device. However, the ISP may be getting their internet delivered through a router supplied by the ISP. In that case, the router allows many devices to use the customer's internet connection and its specifically allocated IP address with other devices connected to it.

This is common in a residential setting. The connected devices can include both wired and wireless devices of many different types: computers, tablets, phones, game consoles, smart TVs, set-top boxes, etc., each of which could be used by different individuals.

[52] In my view, some attempt must be made to determine the internet user responsible for the alleged infringement before a presumption can arise that the internet subscriber is that user or a proper adverse inference can be drawn based on non-responsiveness.

[53] As stated in *Joe Hand Promotions Inc v Social Major League Sports Bar & Grill*, 2009 FC 699 at paragraph 3.

> The practice of using the term "John Doe" in the style of cause is directed at permitting a plaintiff to sue a person whose name the plaintiff does not know. The practice is perfectly acceptable; however, the expectation is that the plaintiff will take reasonable steps to identify the unnamed defendant and then move to amend the style of cause.

[54] The same holds true in this John Doe proceeding with respect to the unnamed defendants and proposed wrongdoers.

[55] In light of the balance the Act seeks to provide between the rights of users and owners (*Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45 [*SOCAN*] at paras 40-41), something more is needed than the bare assertion that a subscriber is, by default, the user responsible for infringement. A direct link must be addressed by the evidence between the internet subscriber and the alleged infringing use or sufficient steps taken for an adverse inference to be drawn against the internet subscriber.

[56] An assumption of infringement is not enough. Based on the steps taken and evidence filed, I cannot conclude that direct infringement by the default internet subscribers has occurred.

[57] While this is sufficient to conclude on this sub-issue, I note that the evidence is also "thin" as to the portions of the Work made available through each IP address. This presents a further evidentiary challenge to be able to conclude that infringement has occurred in each instance. However, in view of my findings above, I need not delve into this further.

(2) Is there Infringement by Authorization?

[58] The leading cases on authorization in the context of copyright infringement are *CCH Canadian Ltd v Law Society of Upper Canada*, 2004 SCC 13 [*CCH*] and *SOCAN*, both of which were decided before the implementation of the notice and notice regime.

[59] *CCH* involved allegations of unauthorized copying from a library photocopier. At paragraph 38, the Supreme Court of Canada considered the meaning of authorization as it related to the use of equipment as follows:

> "Authorize" means to "sanction, approve and countenance": *Muzak Corp. v. Composers, Authors and Publishers Association of Canada, Ltd.*, [1953] 2 S.C.R. 182, at p. 193; *De Tervagne v. Beloeil (Town)*, [1993] 3 F.C. 227 (T.D.). Countenance in the context of authorizing copyright infringement must be understood in its strongest dictionary meaning, namely "[g]ive approval to; sanction, permit; favour, encourage": see The New Shorter Oxford English Dictionary (1993), vol. 1, at p. 526. Authorization is a question of fact that depends on the circumstances of each particular case and can be inferred from acts that are less than direct and positive, including a sufficient degree of indifference: *CBS Inc. v. Ames Records & Tapes Ltd.*, [1981] 2 All E.R. 812 (Ch.D.), at pp. 823-24. However, a person does not authorize infringement by authorizing the mere use of equipment that could

> be used to infringe copyright. Courts should presume that a person who authorizes an activity does so only so far as it is in accordance with the law: *Muzak, supra*. This presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorizer and the person who committed the copyright infringement: *Muzak, supra; De Tervagne, supra; see* also *J.S. McKeown, Fox Canadian Law of Copyright and Industrial Designs* (4th ed. (loose-leaf)), at p. 21-104, and P.D. Hitchcock, "Home Copying and Authorization" (1983), 67 C.P.R. (2d) 17, at pp. 29-33.

[60] In *SOCAN*, Justice Binnie at paragraph 127 commented in *obiter* on what might constitute authorization relating to ISPs before the notice and notice regime:

> The knowledge that someone *might* be using neutral technology to violate copyright (as with the photocopier in the *CCH* case) is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did "(g)ive approval to; sanction, permit; favour, encourage" (*CCH*, at para 38) the infringing conduct. I agree that notice of infringing content, and a failure to respond by "taking it down" may in some circumstances lead to a finding of "authorization". However, that is not the issue before us. Much would depend on the specific circumstances. An overly quick inference of "authorization" would put the Internet Service Provider in the difficult position of judging whether the copyright objection is well founded, and to choose between contesting a copyright action or potentially breaching its contract with the content provider. A more effective remedy to address this potential issue would be the enactment by Parliament of a statutory "notice and take down" procedure as has been done in the European Community and the United States.

[61] The issue of authorization in the BitTorrent framework is currently pending in a proposed reverse class action proceeding involving the Plaintiff and CICC as intervener. A motion to strike the proceeding was recently reversed in part as it related to *inter alia* allegations of authorization by an internet subscriber (*Salna v Voltage Pictures LLC*, 2021 FCA 176 [*Salna*],

leave to appeal to SCC denied, 39895 (26 May 2022)). The FCA provided the following comments at paragraphs 76-85 relating to pleading infringement by authorization:

> [76] The Federal Court also erred in dismissing Voltage's cause of action that the respondents authorized the infringement. The judge concluded that Voltage relied on an overly broad reading of Binnie J.'s *obiter* comment in *SOCAN* at paragraph 127. Binnie J. observed that the failure to take down infringing conduct after receiving notice "*may* in some circumstances lead to a finding of 'authorization'" [Emphasis in original], (Federal Court reasons at para. 79).
>
> [77] Here again, the judge delved into the merits of the argument, rather than considering whether Voltage should be precluded from advancing the argument. At this stage of a proceeding, it is not appropriate to engage in a detailed analysis of the argument, and more particularly, whether the proposed argument is good law (*Merck & Co., Inc. v. Apotex Inc.*, 2012 FC 454, 106 C.P.R. (4th) 325 at para. 28 (*Merck & Co.*)). Indeed, the careful use of the word "may" is an indication from the Court that the question is open for consideration.
>
> [78] When combined, subsections 3(1) and 27(1) of the *Copyright Act* grant the right to authorize the reproduction of a Work. Voltage's claim may push against the boundaries of a claim for authorizing infringement, but that is not the test on a motion to strike. Although the topic of "authorizing infringement" has been judicially considered, the Court in this case is faced with a novel application of the doctrine. Specifically, this Court must consider the prohibition on authorizing infringement in the context of BitTorrent technology and the notice and notice regime.
>
> [79] The key precedents, *CCH* and *SOCAN*, arose in distinct legal and factual contexts. *CCH* dealt with authorization in relation to photocopiers while *SOCAN* was decided prior to the enactment of the notice and notice regime. Accordingly, the extent to which these authorities provide the requisite guidance in this context to conclusively preclude allegations of direct and authorizing infringement at the certification stage is an arguable question.
>
> [80] Mr. Salna made no submissions on the question of whether there was a reasonable cause of action; rather he adopted the argument of the intervener.
>
> [81] CIPICC argues that cases like *CCH*, *SOCAN* and *Century 21* closed the door to the possibility that a party can be liable for

> authorizing infringement without explicitly authorizing infringement. In other words, the mere act of providing access to technology that allowed the infringement cannot on its own ground a claim for authorizing infringement.
>
> [82] CIPICC asks the Court to definitively determine the question of whether, on the facts pled, a reasonable cause of action exists. That is not the role of a court in assessing the reasonableness of a cause of action.
>
> [83] At this stage, all a Court should do is determine whether the moving party should be precluded from advancing their argument in front of a trial judge (*Merck & Co.* at para. 15). In determining this, "[…] the Court must be generous and err on the side of permitting a novel but arguable claim to proceed […]" (*Assn. of Chartered Certified Accountants v. Canadian Institute of Chartered Accountants*, 2011 FC 1516, 2011 CarswellNat 5412 at para. 9; *Merck & Co.* at para. 24). Allowing novel but arguable claims to proceed is the "[o]nly […] way can we be sure that the common law […] will continue to evolve to meet the legal challenges that arise in our modern […] society" (*Hunt v. Carey Canada Inc.*, [1990] 2 S.C.R. 959, 74 D.L.R. (4th) 321 at 990-991). In this instance, Voltage has shown it has a novel but arguable claim.
>
> [...]
>
> [85] It is also clear that Voltage has pled the material facts necessary to support its claim based on a reasonable interpretation of authorizing infringement. For example, as seen in paragraph 44 of the Amended Notice of Application, Voltage pleads that the proposed class members "possessed sufficient control over the use of his or her internet account and associated computers and internet devices such that they authorized, sanctioned, approved or countenanced the infringements particularized herein."

[62] While not necessary at the time of pleading, at the time of adjudication, *Salna* implies that the Plaintiff would have evidence to establish that the internet subscriber "possessed sufficient control over the use of his or her internet account and associated computers and internet devices such that they authorized, sanctioned, approved or countenanced the infringements particularized" (paragraph 85).

[63] In this case, the Plaintiff has not provided any such evidence. Instead, it relies on the comments made in *Rogers* at paragraphs 34 and 35, relating to the deterrent purpose behind the notice and notice regime, which is premised on the capability of an internet subscriber to stop the continuation of copyright infringement by being able to determine who is using the IP address:

> [34] The deterrent purpose of the notice and notice regime also affirms the ISP's duty to correctly determine to whom the impugned IP address belonged at the time of the alleged infringement. Deterring online copyright infringement entails notifying *that* person, because it is only *that* person who is capable of stopping continued online copyright infringement.
>
> [35] I acknowledge that there will likely be instances in which the person who receives notice of a claimed copyright infringement will not in fact have illegally shared copyrighted content online. This might occur, for example, where one IP address, while registered to the person who receives notice of an infringement, is available for the use of a number of individuals at a given time. Even in such instances, however, accuracy is crucial. Where, for example, a parent or an employer receives notice, he or she may know or be able to determine who was using the IP address at the time of the alleged infringement and could take steps to discourage or halt continued copyright infringement. Similarly, while institutions or businesses offering Internet access to the public may not know precisely who used their IP addresses to illegally share copyrighted works online, they may be able, upon receiving notice, to take steps to secure its Internet account with its ISP against online copyright infringement in the future.

[64] The Perino Affidavit asserts that where an ISP's customer is a homeowner getting their internet delivered through a router supplied to the ISP, the homeowner would typically have knowledge of the family members who are connected through the router and there would be limitations to the physical range of the internet connection. Mr. Perino notes that almost all routers provide security settings that "allow a password to be put on Wi-Fi access, enable a blacklist to ban specified devices, enable a whitelist to only permit specified devices and block certain types of internet traffic (such as BitTorrent)." The Plaintiff contends from this evidence

that the Default Defendants could have easily taken action to prevent infringement by; for example, changing the Wi-Fi passwords, blacklisting unauthorized devices or even blocking the BitTorrent protocol.

[65] CIPPIC argues that the Plaintiff seeks to lower the standard of authorization to whether the alleged authorizer has any power to *stop* the direct infringer. They assert that this is akin to the standard adopted in Australia, which the Supreme Court explicitly rejected in *CCH* when it stated at paragraphs 39-41:

> ... At trial, the Law Society applied for a declaration that it did not authorize copyright infringement by providing self-service photocopiers for patrons of the Great Library. No evidence was tendered that the photocopiers had been used in an infringing manner.
>
> The trial judge declined to deal with this issue, in part because of the limited nature of the evidence on this question. The Federal Court of Appeal, relying in part on the Australian High Court decision in *Moorhouse v. University of New South Wales*, [1976] R.P.C. 151, concluded that the Law Society implicitly sanctioned, approved or countenanced copyright infringement of the publishers' works by failing to control copyright and instead merely posting a notice indicating that the Law Society was not responsible for infringing copies made by the machine's users.
>
> With respect, I do not agree that this amounted to authorizing breach of copyright. *Moorhouse*, *supra* is inconsistent with previous Canadian and British approaches to this issue. See D. Vaver, *Copyright Law* (2000), at p. 27, and McKeown, *supra*, at p. 21-108. In my view, the *Moorhouse* approach to authorization shifts the balance in copyright too far in favour of the owner's rights and unnecessarily interferes with the proper use of copyrighted works for the good of society as a whole.

[66] As noted by CIPPIC, even under the more liberal Australian standard, the relevant statutory provision provides for consideration to be given to the extent to which the proposed authorizer has power to prevent the doing of the act concerned, the nature of the relationship

between the proposed authorizer and infringer, and whether reasonable steps were taken to prevent or avoid the act (*Copyright Act*, (Austl), 1968/63, section 36(1A)).

[67] While *Salna* indicates that the door should not be closed to evolving the law relating to authorization in order to meet the needs of modern technology, there must still be a balanced approach. If one were to apply the Plaintiff's argument to this action, this would mean that once an internet subscriber is notified of a potential infringement under the notice and notice regime, if the infringement does not cease, they would be liable for authorizing the infringement without the need to establish any control or relationship to the infringer. In my view, this lowers the bar and tips the balance under the Act in favour of copyright owners.

[68] To establish authorization in this context, in my view, consideration must be given to not only whether the Default Defendant had knowledge of the alleged infringing activity, but also the relationship and extent of control over the user and whether the internet subscriber had some ability to prevent the act of concern.

[69] The Plaintiff provided notices to the Default Defendants through their ISPs, who confirmed that the notices were sent. The confirmations that the emails were sent is sufficient to ground a presumption that the notices were received by the internet subscribers (*Zare v Canada (Minister of Citizenship and Immigration)*, 2010 FC 1024 at para 48) and that they had knowledge of the alleged infringing activity.

[70] However, there is no evidence as to the nature of relationship between the internet subscribers identified as Default Defendants and those that actually uploaded the unauthorized content, who as discussed earlier have not been identified. There is also no evidence as to what steps, if any, the internet subscribers have taken to prevent further alleged infringement. As previously noted, some form of discovery could be sought to seek these facts or any others that would support a finding of authorization or allow an adverse inference to be drawn.

[71] On the basis of the record before me, there is insufficient evidence to ground a finding of infringement by authorization.

(3) Other Allegations - Is there Secondary Infringement

[72] While not argued orally, the Plaintiff's written representations also assert that the Default Defendants have engaged in secondary infringement. This presents an even steeper hurdle for the Plaintiff from an evidentiary stand-point.

[73] In order to establish secondary infringement under subsection 27(2) of the Act, the following test must be satisfied (*CCH* at para 81*; Euro-Excellence v Kraft Canada Inc*, 2007 SCC 57; *Salna* at para 87): a) there must be an act of primary infringement; b) the secondary infringer must be shown to have known that he or she was dealing with a product of infringement; and c) the secondary infringer must have sold, distributed or exposed for sale the infringing goods.

[74] I agree with CIPPIC that there is insufficient evidence to establish secondary infringement. In particular, the Plaintiff has not provided any evidence that the Default Defendants have committed any of the acts specified in the third part of the test – that is, that they have sold, distributed or exposed the Work for sale either directly or by authorization.

[75] Accordingly, judgment cannot issue on the basis of this further allegation.

## IV. Remedies and Conclusion

[76] Given my findings on the infringement issue, I need not go on at this stage to consider the statutory damages requested.

[77] Rule 210(4) provides that the Court may on a motion for default judgment do one of three things: a) grant judgment; b) dismiss the action; or c) order that the action proceed to trial and that the plaintiff prove its case in such a manner as the Court may direct.

[78] On the basis of the evidentiary deficiencies noted, I cannot grant judgment. Nor am I prepared to find that the Plaintiff would not be entitled to any relief for its claim on a more fulsome evidentiary record. Accordingly, I shall invoke Rule 210(4)(c) and the Plaintiff shall be ordered to requisition a case management conference to set the next steps to advance the case to trial. The order shall be made without prejudice to the Plaintiff's ability to seek default judgment again on a different evidentiary record that addresses the deficiencies noted in these reasons.

**ORDER IN T-513-18**

**THIS COURT'S ORDER is that**

1. The motion for Default Judgment is dismissed.

2. The action shall proceed forward to trial pursuant to subrule 210(4)(c).

3. The Plaintiff shall within thirty (30) days of the date of this Order requisition a case management conference to set a timetable for the next steps in the action.

4. Notwithstanding paragraph 2, the Plaintiff is not precluded from commencing a further motion for default judgment on a different evidentiary record that addresses the deficiencies noted in these reasons.

5. This is no order as to costs.

"Angela Furlanetto"
Judge

**Schedule "A"**

| Default Defendant | IP Address |
|---|---|
| Doe #3 | 142.162.128.245 |
| Doe #4 | 47.54.165.90 |
| Doe #8 | 99.192.57.154 |
| Doe #15 | 142.167.107.117 |
| Doe #18 | 67.68.98.171 |
| Doe #20 | 76.68.210.170 |
| Doe #23 | 65.93.22.84 |
| Doe #24 | 65.93.37.104 |
| Doe #26 | 174.95.209.150 |
| Doe #30 | 70.54.41.122 |
| Doe #33 | 76.68.165.22 |
| Doe #36 | 67.70.141.111 |
| Doe #37 | 174.89.225.185 |
| Doe #42 | 76.64.239.125 |
| Doe #48 | 184.145.217.50 |
| Doe #49 | 70.30.248.51 |
| Doe #50 | 70.51.141.35 |
| Doe #51 | 65.92.23.220 |
| Doe #58 | 70.30.252.247 |
| Doe #62 | 174.95.184.185 |
| Doe #63 | 184.144.235.232 |
| Doe #66 | 174.95.132.108 |
| Doe #84 | 174.113.26.41 |
| Doe #86 | 174.115.198.172 |
| Doe #93 | 174.112.229.30 |
| Doe #94 | 99.255.192.147 |
| Doe #97 | 99.248.153.126 |
| Doe #103 | 99.239.4.175 |
| Doe #108 | 99.243.10.135 |
| Doe #109 | 99.224.179.37 |

**FEDERAL COURT**

**SOLICITORS OF RECORD**

| | |
|---|---|
| **DOCKET:** | T-513-18 |
| **STYLE OF CAUSE:** | VOLTAGE HOLDINGS, LLC v DOE#1 ET AL (SEE SCHEDULE 1 FOR LIST OF DEFENDANTS) AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC |
| **PLACE OF HEARING:** | HEARD BY VIDEOCONFERENCE |
| **DATE OF HEARING:** | NOVEMBER 29, 2021 |
| **JUDGMENT AND REASONS:** | FURLANETTO J. |
| **DATED:** | JUNE 6, 2022 |

**APPEARANCES:**

| | |
|---|---|
| Kenneth R. Clark<br>Lawrence Veregin | FOR THE PLAINTIFF |
| David A. Frewer | FOR THE INTERVENER |

**SOLICITORS OF RECORD:**

| | |
|---|---|
| Aird & Berlis<br>Barristers and Solicitors<br>Toronto, Ontario | FOR THE PLAINTIFF |
| Samuelson-Glushko & Public Interest Clinic<br>University of Ottawa, Faculty of Law. Common Law Section<br>Ottawa, Ontario | FOR THE INTERVENER |