Rethinking online privacy in Canada: commentary on Voltage Pictures v. John and Jane Doe

Ngozi Okidegbe[*]

INTRODUCTION

In the recent *Voltage*[1] decision, the Canadian Federal Court affirmed that the *bona fide* standard is the legal standard required for a court to order a third-party online service provider to disclose subscriber information to a copyright owner. On this basis, the Federal Court ordered an Internet Service Provider (ISP) to disclose the identities of roughly two thousand subscribers alleged to have illegally shared the plaintiff's copyrighted works. This *bona fide* standard was satisfied by evidence linking the IP addresses involved in the illegal file sharing to subscribers of the ISP. This decision affirmed that disclosure orders can be obtained solely by producing evidence linking the IP addresses assigned to an ISP with illegal file sharing, a holding that had been set by the Canadian Federal Court of Appeal in *BMG*.[2] While this decision provides copyright owners with an effective tool to protect their intellectual property rights, it also affords a relatively low threshold of protection for the personal information of ISP account holders, one that falls below their reasonable expectations of privacy.

This article examines the *Voltage* decision, with the view that the *bona fide* standard safeguards intellectual property rights at the cost of online privacy rights and will proceed in three parts. Part I provides a brief contextualization of the issues. Part II is an analysis of the *Voltage* decision. Part III examines how the *bona fide* standard is a relatively low threshold. This article concludes by considering the possibility of shifting to a higher standard for disclosure, as well as a possible solution for the effect that a higher standard could have on copyright owners.[3]

I. CONTEXTUALIZATION

This section discusses three issues: (a) the occurrence of online piracy on peer-to-peer (P2P) networks; (b) the process by which copyright owners currently

---

* BCL/LLB Candidate, McGill Faculty of Law. The author thanks Dr. Sunny Handa and Professor David Lametti for their feedback with respect to this article. She also thanks Mr. Philip Brink for research assistance.

1 *Voltage Pictures LLC v. John Doe*, 2014 FC 161, 2014 CarswellNat 1599, 2014 CarswellNat 1600 (F.C.) [*Voltage*].

2 *BMG Canada Inc. v. John Doe*, 2005 CarswellNat 1300, 2005 CarswellNat 4969, 2005 FCA 193 (F.C.A.) [*BMG*].

3 The implications of requiring a higher standard of disclosure in criminal cases are beyond the scope of this article.

enforce their copyright infringement claims; and (c) the privacy rights that are at stake in these instances.

(a) Piracy on P2P Networks

Canada is ranked tenth in the world for online piracy of copyrighted material.[4] The most prominent form of online piracy today involves illegal file sharing over P2P networks using a file-transfer protocol named BitTorrent.[5] Users of BitTorrent will generally search a torrent indexing website that provides links to the specific content that they wish to obtain. The user will then download the desired files from "seeders," which is a term for users that are sharing complete works on the network, and "peers," which is a term for users who are also downloading the same torrent, and are sharing the portions which they have already downloaded on the network. During the download, the user will be a peer, and will share completed portions of the torrent with others, and upon the completion of the download, the user automatically becomes a seeder. Until the user removes the file from his or her BitTorrent client, the user will be a seeder for subsequent downloaders.[6] The popularity of BitTorrent comes from the fact that it provides a user fast and easy access to media files such as music, books, and movies. While the majority of the files shared are copyrighted material,[7] the BitTorrent protocol is also an important method of distribution for many free and open-source content providers.[8]

(b) Legal Enforcement of Copyright Claims

To litigate their copyright infringement claims, copyright owners must track the IP addresses involved and apply for a *Norwich*[9] order so as to compel third-party ISPs to disclose the personal identities of their clients who were using these IP addresses. This is only granted where the court is satisfied that: (1) the plaintiff has a *bona fide* case against the proposed defendants; (2) the third party has information pertaining to an issue in the proceeding; (3) disclosure is the only reasonable means of obtaining the information; (4) fairness requires that the information be provided prior to trial; and (5) the order made will not cause undue delay, inconvenience, or expense to the third party or others.[10]

---

4 BayTSP, *Annual Report Online Trends & Insight* (Los Gatos: BAYTSP, 2008) at 6, online: <http://tech.mit.edu/V129/N28/piracy/BayTSP2008report.pdf>.

5 Paul A. Watters et al, "How Much Material on BitTorrent is Infringing Content?: A Case Study" (2011) 16 Information Security Technical Report 79 at 86.

6 For more information about the nature of BitTorrent, see Matteo Varvello et al, "Understanding Bit-Torrent: A Reality Check From the ISP's Perspective," (2012) 56 *Computer Networks* 1056; Justin Bieber et al, *An Empirical Study of Seeders in BitTorrent* (Durham: Duke University, 2006); Carmen Carmack, "How BitTorrent Works", online: HowStuffWorks <http://computer.howstuffworks.com/bittorrent.htm>.

7 Watters, *supra* note 5 at 86.

8 Chao Zhang, "Unraveling the BitTorrent Ecosystem" (2011) 22 IEEE Transactions on Parallel and Distributed Systems 1164 at 1164.

9 *Norwich Pharmacal Co. v. Customs & Excise Commissioners*, [1974] A.C. 133 (U.K. H.L.).

10 *Voltage*, *supra* note 1 at para 45.

These criteria are easily satisfied where the order pertains to online copyright infringement. First, copyright owners are often able to show that they have a *bona fide* case against the proposed defendants, by presenting evidence linking IP addresses connected to the copyright infringement with the subscribers of the ISP. Second, the ISP commonly has information pertaining to the identities behind these IP addresses. Third, disclosure is the only reasonable method by which a copyright owner can obtain the information. Fourth, the fact that copyright owners are often ordered to cover expenses related to compliance with *Norwich* orders generally means that such orders will not be deemed to cause delay, inconvenience, or expense to the ISP. Though *Norwich* orders are granted without any consideration of online privacy rights, they are subject to judicial supervision for the purpose of preventing copyright owners from abusing the process.[11]

(c) Online Privacy Rights

ISP account holders have privacy rights that are guaranteed by the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[12] This federal statute protects users by prohibiting ISPs from disclosing their personal information without consent or a court order, thereby affording users a reasonable expectation of privacy.[13] The notion that internet users have a reasonable expectation of privacy was recently affirmed by the Supreme Court of Canada in *Spencer*.[14] That case concerned the constitutionality of the police obtaining an account holder's subscriber information from his ISP without prior judicial authorization, on the basis that the holder's IP address was involved in child pornography. The police had relied on section 7(3)(c.1)(ii) of *PIPEDA* which they contended gave them the authority to compel the ISP to disclose such information. The Supreme Court disagreed with this viewpoint, holding that an ISP must disclose such information only if required by a court order and thus the police action was unconstitutional.[15] In reaching this decision, the Court articulated that Internet users have a reasonable expectation of privacy with respect to their Internet browsing activity and subscriber information.[16] This was characterized as an "informational privacy" interest, which included a reasonable expectation to: (1) secrecy as to the content of Internet browsing activity; (2) control over the access to and use of such information; and (3) anonymity.[17] Although the case was decided under section 8 of the

---

11 This concern is related to copyright trolling. For more information about copyright trolling, see Sean B. Karunaratne, "The Case Against Combating BitTorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits" (2012) 111 Michigan Law Review 283 at 285; see also, Gregory S. Mortenson, "BitTorrent Copyright Trolling: A Pragmatic Proposal for a Systemic Problem" (2013) 43 Seton Hall L. Rev 1105.

12 *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 ["PIPEDA"].

13 *Ibid* at ss 3,7.

14 *R. v. Spencer*, 2014 SCC 43, 2014 CarswellSask 342, 2014 CarswellSask 343 (S.C.C.) [*Spencer*].

15 *Ibid* at paras 71–74.

16 *Ibid* at para 66.

17 *Ibid* at paras 37-38, 40–43,45.

Canadian *Charter*,[18] the Court provided a strong endorsement as to the existence and substance of an internet user's online privacy rights. While a right to privacy is neither an absolute right nor a shield against wrongdoing, the *Spencer* decision affirms the strong public interest in protecting online privacy rights from unjustified interference.

II. THE VOLTAGE DECISION

The plaintiff was a film company named Voltage Pictures, which discovered that its films were being illegally copied and downloaded over P2P networks in Canada. The company then retained the services of Canipre to identify and collect the IP addresses involved. The IP addresses were assigned by an ISP known as TekSavvy Solutions. Pursuant to this evidence, Voltage Pictures filed a *Norwich* order requesting disclosure of the names and addresses of the approximately 2000 subscribers involved. TekSavvy Solutions did not oppose the motion. However, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC") intervened on the basis that the legal standard for such a disclosure order should be a *prima facie* case. Under this proposed standard, IP address evidence would not be sufficient to merit disclosure, due to its unreliability in ascertaining the identity of the actual copyright infringer. Voltage Pictures, therefore, would have to provide further evidence in order to be granted a *Norwich* order.

(a) Judicial Reasoning

The Federal Court ruled in favor of Voltage Pictures. First, the Court affirmed that the *bona fide* standard was the correct legal standard for granting a *Norwich* order. In this respect, the Court found itself bound by the *BMG* decision, which held that requiring a higher standard would be an insurmountable burden for copyright owners.[19] Without having the identities of the proposed defendants, the *BMG* Court held that it would be impossible for copyright owners to demonstrate a *prima facie* case, which the *Voltage* Court reaffirmed.[20] Second, the *Voltage* Court also held that Voltage Pictures had satisfied the *bona fide* standard by producing evidence demonstrating that TekSavvy Solutions had assigned the IP addresses connected to the copyright infringement. Though recognizing that evidence consisting solely of IP addresses was unreliable, the Court determined that there was no other way that Voltage Pictures, or any copyright owner, could otherwise link the subscribers of an ISP to illegal file sharing. The Court also placed a number of restrictions on the disclosure order, so as to accommodate the privacy rights of ISP account holders. These included that the order must: (1) not include the e-mail addresses or telephone numbers of the subscribers; (2) place a legal obligation on Voltage Pictures to keep the disclosed information confidential and to use the information only within the purview of judicial oversight; and (3) that the Court would reserve the right to order amendments to any demand letters granted or actions

---

18 *Canadian Charter of Rights and Freedoms*, s 8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 [*Charter*].

19 *BMG*, *supra* note 2 at para 34.

20 *Voltage*, *supra* note 1 at para 39.

taken.[21] According to the Court, the imposition of these restrictions properly balanced the privacy rights of ISP account holders with the rights of copyright owners.

III. PROBLEMS WITH THE BONA FIDE STANDARD

Though the *Voltage* Court accepted that the *bona fide* standard could be satisfied by evidence linking IP addresses to the subscribers of an ISP, this decision failed to consider the substantial unreliability of such evidence. To understand this problem, it is important to recognize the reasons why IP addresses are unreliable. The first reason is rooted in the process by which IP addresses are assigned. Each ISP has a block of IP addresses from the American Registry for Internet Numbers that it temporarily assigns to an account holder every time that he or she connects to the Internet.[22] The same IP addresses can be allocated to several different users over the course of a single day. Unless an ISP has an infrastructure that maintains records of every IP address assigned to each account user for an extended period of time, the process of determining the account holder assigned to an IP address at a specific time becomes increasingly unreliable the older the information becomes.[23]

The second reason for the unreliability of such evidence is even when an ISP maintains such an infrastructure, there is nothing in the IP address that can identify the individual person committing copyright infringement. Courts around the world are becoming increasingly aware of this fact. In the United Kingdom case of *Media Cat.*, this factor was used to dismiss a copyright infringement claim brought by a copyright owner.[24] In that case a law firm brought an action on behalf of a copyright owner and successfully obtained a disclosure order against 27 defendants on the basis of their IP addresses being linked to the illegal file sharing of pornographic films over P2P networks. In dismissing the case, Judge Birss held that linking an account holder to an IP address involved in copyright infringement does not establish that the owner of that account was the person who committed the copyright infringement. He stated that, "Proof that a person owns a photocopier does not prove they have committed acts of copyright infringement."[25] This same reasoning can be seen in current jurisprudential trends in the U.S., most recently in the decisions of *Malibu*[26] and *AF*.[27] Both cases concern copyright owners subpoenaing ISPs for the personal information of subscribers whose IP addresses had been connected to illegal file sharing of their copyrighted works. Both courts quashed the subpoenas on the basis of the unreliability of IP addresses as proof of copyright infringement. The *Malibu* Court found that, "There is nothing that links the IP ad-

---

21 *Ibid* at pp. 56–58.

22 For more information, see the American Registry for Internet Numbers website online: <https://www.arin.net/about_us/overview.html>.

23 *BMG Canada Inc. v. John Doe* , 2004 CarswellNat 2774, 2004 CarswellNat 835, 2004 FC 488 (F.C.), at para 33.

24 *Media CAT Ltd. v. Adams & Ors*, [2011] EWPCC 6.

25 *Ibid* at para 7.

26 *Malibu Media v. John Doe*, [2014] US District Court Southern District of Florida, Case No. 1:14-cv-20213-UU.

27 *AF Holdings v. John Doe*, [2012] US District Court Central District of California, Case No. 2:12-cv-5709-ODW(JCx).

dress location to the identity of the person actually downloading and viewing [the] Plaintiff's videos[.]"[28] Furthermore, it held, "[T]he geolocation software cannot identify who has access to that residence's computer and who would actually be using it to infringe [the] Plaintiff's copyright."[29] Similarly the Court in the *AF* case held that:

> An IP address alone may yield subscriber information, but that may only lead to the person paying for the Internet service and not necessarily the actual infringer, who may be a family member, roommate, employee, customer, guest, or even a complete stranger.[30]

Both of these decisions demonstrate a trend of refusing evidence consisting only of IP addresses as a basis for allowing disclosure orders. Unlike the *Voltage* Court, neither of these U.S. courts found that placing restrictions on how the disclosed information could be utilized by the copyright owner compensated for the privacy risks rooted in the unreliability of the evidence.

The third reason for the unreliability of IP addresses is the widespread availability of unprotected networks. For instance, many coffee shops, Internet cafés, and home residences do not have password-protected networks. Even where coffee shops and Internet cafés do have password-protected networks, they often have not installed the security software required to monitor and prevent piracy on their networks. In addition, Wi-Fi connections can be hacked, and thus copyright infringement can occur on a network without either the authorization or the knowledge of the account holder — particularly if their account is protected by a weak password or WEP encryption methods.[31]

All of these reasons demonstrate the serious risks of relying solely upon the evidence of IP addresses for *Norwich* orders. It also shows that the *bona fide* standard does little to prevent innocent users from having their personal information disclosed, the consequences of which extend far beyond their names and addresses being revealed to a copyright owner.[32] *Ex parte* orders may compel the seizure of a user's computer(s) in order to preserve potential evidence. In many instances, large amounts of personal information on their hard drives are searched by the authorities. These consequences occur in spite of the fact that the innocent user may not have pertinent information leading to the true infringer. In addition, the innocent user will likely face high legal costs from defending against such allegations. It is difficult to justify exposing a potentially innocent person to such a substantial interference of his or her privacy, solely on the evidentiary basis of an IP address — particularly where the subsequent consequences of such disclosure cannot be miti-

---

28 *Malibu*, *supra* note 27 at 1.

29 *Ibid* at 2.

30 *AF*, *supra* note 28 at 1–2.

31 For more information, see Nancy Cam-Winget, "Security Flaws in 802.11 Data Link Protocols" (2003) 46 Communications of the ACM 35.

32 For more information, see Amy Min-Chee Fong, "Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners" (2005) 4 CJLT 169.

gated by judicial oversight.[33] This demonstrates the relatively low threshold that the *bona fide* standard affords for the protection of privacy rights.

With the use of IP addresses as a basis for satisfying the *bona fide* standard, the risk of innocent ISP account holders being ensnared in a disclosure order, and thereby having their privacy violated, are substantial. If *Norwich* orders were issued according to a higher standard, such as the *prima facie* standard, such a result would be less likely to occur, as copyright owners would have to prove a *prima facie* case before obtaining such an order. This would require them to produce further evidence of copyright infringement in addition to IP addresses, which would decrease the chances of ensnaring innocent users and be consistent with the trend developing in the U.K. and U.S.

IV. IMPLICATIONS OF A PRIMA FACIE STANDARD

Arguably, applying a higher legal standard for the issuing of a *Norwich* order could make it harder for copyright owners to obtain disclosure orders, a requirement for litigating their rights at court. However, the protection of intellectual property rights should not have to come at the expense of the privacy rights of ISP account holders. This is especially true due to the fact that there are other potential options for copyright owners to pursue their claims outside of a civil proceeding. One promising option is based on the Copyright Alert System, which is currently in effect in the United States. The Copyright Alert System was created by a 2011 agreement[34] between copyright owners and major ISPs.[35] This enforcement mechanism functions entirely without state intervention. Under this system, copyright owners inform an ISP of IP addresses connected with copyright infringement. The ISP is then contractually obligated to first warn the account holder of his or her alleged infringement. After five complaints of infringement have been received about the same account, the ISP then must choose from one of the following options: (1) throttling the account holder's connection speed; (2) stepping down the account holder's service tier; (3) temporarily suspending their internet service; or (4) terminating their Internet service. The agreement provides for a private review proceeding with an "independent reviewer,"[36] through which an account holder can contest the disciplinary action taken against them.[37]

---

33 The *Voltage* Court was persuaded that judicial oversight mitigated the consequences of a *Norwich* order on the privacy rights of ISP account holders; *Voltage*, *supra* note 1 at paras 133 and 134.

34 The agreement is called the Memorandum of Understanding, see Center for Copyright Information, *Memorandum of Understanding*, online: Center for Copyright Information <http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf>.

35 AT&T, Verizon, and Time Warner are among the signatories.

36 Center for Copyright Information, *supra* note 37 at 31, 33, 35.

37 Arguably, the independent reviewer is appointed indirectly by the copyright owners and ISPs because Memorandum of Understanding provides for the independent reviewer to be appointed by a "panel of neutrals" selected by the Administering Organization, which is itself appointed by a six member executive committee consisting of three members designated by the copyright owners and three members designated by

There are two clear weaknesses with this system: the potential loss or throttling of an internet connection for account holders found to have engaged in copyright infringement, and the lack of guarantee that the appeal process will be procedurally fair or conform with the principle of due process. These weaknesses can be ameliorated through significant modifications to the system. The first modification should be to eliminate the prospect of throttling or loss of internet service, and instead to institute a fine.[38] Not only is a fine more proportionate with the nature of the offence, it is also more in line with the importance our society places on access to the Internet. The Internet has become fundamental to how we participate in society, and thus should not be denied to a user solely due to six counts of copyright infringement. In addition, the denial of internet access should only be possible through a court order as opposed to any private agreement between ISPs and copyright owners. The second modification should be to place the appeal process within the purview of a governmentally-mandated administrative tribunal.[39] Assessing alleged copyright infringements and evaluating the merits of any defense that would be put forth by alleged infringers falls outside the competency of ISPs and copyright owners. Putting the process within the purview of an administrative tribunal would alleviate the concerns associated with ISPs and copyright owners policing copyright enforcement, particularly with respect to the ability of those actors to be neutral. An administrative tribunal thus ensures that account holders would receive a fair hearing that adheres to the principles of due process and procedural fairness.

With these modifications, this system would strike a fairer balance between privacy rights and intellectual property rights in copyright infringement cases. This method would better protect online privacy rights because ISPs themselves would be responsible for the notification and penalization of account holders suspected of copyright infringement. This means there would be fewer instances in which subscriber information would be released to copyright owners. For account holders who are potentially innocent of any copyright infringement, this method would provide them with an opportunity to respond to the allegations without the consequences associated with a civil proceeding.[40] It also would allow the account holder to take measures in order to prevent the risk of such complaints in the future, an ability that does not exist with the current copyright enforcement system. In addition, it would also protect the rights of copyright owners by penalizing those who wilfully engage in copyright infringement.

V. CONCLUSION

The *Voltage* decision demonstrates the need to rethink the protection that is currently afforded to online privacy rights in copyright enforcement cases. The cur-

---

the participating ISPs. The review itself requires the user to pay a 35 dollar filing fee, see *ibid* at 33.

38 This is the modification advocated by Danielle Serbin in "The Graduated Response: Digital Guillotine or a Reasonable Plan for Combating Online Piracy?" 3 Intellectual Property Brief 42 at 51.

39 This is the modification advocated by Rachel Storch, in "Note: Copyright Vigilantism" (2013) 16 Stan Tech L Rev 453 at 479–483.

40 Storch, *supra* note 42 at 469.

rent usage of the *bona fide* standard in granting *Norwich* orders provides little safeguard for the reasonable expectation of privacy that internet users hold and that the *Spencer* Court affirmed. The facts that gave rise to the *Voltage* case provided a perfect opportunity to address and rectify this problem, an opportunity that was missed by the *Voltage* Court. Rather than grappling with the serious privacy implications involved with the granting of a *Norwich* order, the Court prioritized intellectual property rights at the expense of affording adequate protection to the right to online privacy. In the future, we must adopt the *prima facie* standard in *Norwich* orders and consider implementing a modified Copyright Alert System so as to ensure that both intellectual property rights and online privacy rights are safeguarded.