

# Don't shoot the messenger!

## Is there liability for intermediaries for online gambling?

BY C. IAN KYER AND ANDREW ALLEYNE

*"Internet liability is... a vast field where the legal harvest is only beginning to ripen." – Justice Binnie in Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers (SOCAN).*



### Intermediaries as Attractive Defendants

When the United States began its campaign against online gambling, Internet intermediaries, telecommunications providers and Internet service providers (ISPs), became nervous. Would they be caught in the net of anti-gambling measures? Although some time has gone by, the question remains largely unanswered. Internet intermediaries are the sine qua non of the online gambling industry. Without the wired and wireless services that these intermediaries offer, Canadians could not access offshore gambling sites and engage in online gambling. However, unlike online gambling companies, intermediaries offer a more easily accessible target as their head offices and bank accounts are located in Canada and, in some cases, they have very deep pockets. For all of these reasons, intermediaries are legitimately concerned about possible criminal and civil liability.

### "Here and There": The Ability of Canadian Courts to Assume Jurisdiction

Though there is no instance of Canadian courts assuming jurisdiction in a case dealing specifically with the liability of Internet intermediaries regarding online gambling activities undertaken using their services,<sup>2</sup> there are precedents that deal with cross-border telephone fraud, defamation, and copyright infringement that would likely allow Canadian courts to assume jurisdiction in such a case.<sup>3</sup> With regard to telecommunications in general, Canadian courts have taken the position that there may be a "real and substantial connection"<sup>4</sup> in matters of civil and criminal liability regarding foreign transmissions coming into Canada<sup>5</sup> and transmission from Canada to other jurisdictions.<sup>6</sup> American courts have taken a similar view in assuming jurisdiction both when the US is the country of transmission<sup>7</sup> and when it is the country of reception.<sup>8</sup>

While it dealt with an online gambling company rather than an Internet intermediary, the *R. v. Starnet Communications International Inc.*<sup>9</sup> decision underscores that an online gaming operation that is unlicensed in Canada but has sufficient connections to Canada may still be successfully prosecuted under the *Criminal Code*. Ultimately, to relieve itself of criminal liability, Starnet had to restructure itself in a manner that reduced its connections to Canada significantly. From *Starnet*, it is apparent that relevant connecting factors—and therefore potential targets for

prosecution—might include the end users, the gaming operator, the host server, and the intermediaries. Given the amorphous multi-jurisdictional nature of online gambling companies and the anonymous nature of the Internet, it becomes immediately apparent that it might be difficult to pursue the gaming operator and to properly identify the end users. This leaves Internet intermediaries—those that may be hosting the online gambling website on their servers and whose customers may be using their infrastructure to access the online gambling website—as the most readily available targets for legal action. The possible willingness of Canadian courts to assume jurisdiction based on both transmission and reception of telecommunications only broadens the potential number of intermediaries that might be added as parties to a lawsuit.

### **The Knowledge Factor for Criminal Responsibility: Controlling the Medium but not the Message<sup>10</sup>**

A foundational principle of criminal justice in common law jurisdictions is that an act cannot make a person guilty unless their mind is also guilty. Thus, in addition to fault, in order to be found criminally guilty an awareness of wrongdoing is required in Canada for any type of offence with the possibility of imprisonment,<sup>11</sup> such as the *Criminal Code's* gambling provisions.<sup>12</sup> Although it is clear that some sort of knowledge of illegal activity would be required for Internet intermediaries to be held criminally responsible, the lack of case law specifically dealing with intermediary liability in the online gambling context makes it difficult to determine what would constitute such knowledge. Given the

uncertainty about what is legal and illegal in the online gambling context, would it be unfair to expect our intermediaries to police the offerings made through their services in order to avoid liability?

### **Turning to Other Common Law Jurisdictions for Guidance**

Because of the dearth of Canadian legislation and case law dealing with intermediary liability in the online gambling context, it is helpful to turn to the US and the UK for guidance. Despite the US' strong stance against online gambling, there are several key instances where their legislation insulates Internet intermediaries from liability. Section 230(c)(1) of the *United States' Communications Decency Act* of 1996<sup>13</sup> states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Further, s. 2 of the *Unlawful Internet Gambling Enforcement Act*<sup>14</sup> of 2006 states that "the term 'business of betting or wagering' does not include the activities of a financial transaction provider, or any interactive computer service or telecommunications service." Though not binding in Canada, the fact that the US, even with its vigorous anti online gambling campaign, has legislation aimed at protecting intermediaries, gives some indication as to how a Canadian court might decide an intermediary liability case.

In a recent UK decision,<sup>15</sup> the court addressed intermediary liability in the defamation context. The judge explained that "an ISP which performs no more than a passive role in facilitating postings on the internet cannot be deemed to be a publisher at common law." However, that, if it can

be proven that the ISP "knowingly permits another to communicate information which is defamatory, when there would be an opportunity to prevent the publication, there would seem to be no reason in principle why liability should not accrue."<sup>17</sup> If there were to be an intermediary liability case in the online gambling context in Canada, it is likely that, as in this UK defamation case, it would turn on the issue of knowledge.

### **Guidance from Canada?**

Although we have no Canadian cases that have dealt specifically with the criminal accountability of intermediaries for facilitating illegal online gambling in Canada, we have a number of cases where our courts have looked at their responsibility for other illegal acts, such as copyright infringement, which may be of some precedent value. Those cases suggest that mere passive transmission of unknown content will not create liability. Those same cases suggest that there is a line between such activity and knowingly promoting the illegal activity.

### **The Ability of the Intermediary to Control the Offender**

Though not dealing with Internet intermediaries, several older cases provide some insight into the level of authorization that is acceptable. These cases focus on the ability of the intermediary to exercise control over the infringing party and directly prevent infringement. In one case, the court explained that "authorize" must be interpreted to mean "sanction approve and countenance" the infringing act.<sup>18</sup> This focus on the ability of the intermediary to control the infringer persists in contemporary Canadian case law. In one instance,<sup>19</sup> a play was publicly

performed at a non-profit community centre without the consent of the copyright holder. After the producer filed for bankruptcy, the copyright holder pursued an action against the community centre as the intermediary. The court ruled that the community centre exercised no control over the producer and, therefore, did not authorize the performance within the meaning of the *Copyright Act*.<sup>20</sup> If there was a formalized agreement where the community centre had direct control over the producer, such as an employment agreement, the court suggested that such authorization might have been deemed to occur. This would seem to suggest that an intermediary that merely passively hosts an online gambling website—without any formal agreement that allows them to control their clients’ activities—would not be seen as authorizing illegal behaviour. However, intermediaries often require the websites they host to sign agreements which include indemnity provisions and terms of use that provide that the intermediary will cease hosting the website if there is evidence of illegal activity. The inclusion of such terms might imply a certain degree of control, and hence liability.

### **Only Authorized in Accordance with the Law**

More recently, in *CCH Canadian Ltd. v. Law Society of Upper Canada*,<sup>21</sup> the Supreme Court clarified that in addition to control, to the extent that implied authorization is provided, this authorization does not encompass illegal activities. Here, the copyright owners claimed that the Law Society was responsible for infringement occurring at the Great Library at Osgoode Hall as they made photocopying services

available to library patrons. Chief Justice McLachlin, writing on behalf of the Court, emphasized that “a person does not authorize infringement by authorizing the mere use of equipment that could be used to infringe copyright.”<sup>22</sup> However, she added, “this presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorizer and the persons who committed the copyright infringement.”<sup>23</sup> Therefore, assuming the logic of *CCH* could be extended to intermediaries in the online gambling context, if there is no formal relationship whereby an intermediary could exercise control over the activities of an online gambling website, it is presumed that any illegal activities conducted over this website would not be seen as authorized by the intermediary. However, once made aware of illegal activities, the protections of *CCH* will likely no longer apply.

### **Ignorance is Bliss: Passive Retransmitters**

An early approach taken by the Supreme Court of Canada<sup>24</sup> focuses on the intermediary’s lack of knowledge of the transmission as the key factor allowing it to avoid liability. The court reasoned that “the owners of the telephone wires, who are utterly ignorant of the nature of the message intended to be sent, cannot be said within the meaning of the covenant to transmit a message of the purport of which they are ignorant.”<sup>25</sup> This same logic prevailed 113 years later in the *SOCAN* case.<sup>26</sup> In *SOCAN*, the plaintiffs alleged that the ISPs were not merely passive conduits for information of which they had no knowledge, but active participants in copyright infringement.<sup>27</sup>

The ISPs, however, maintained that although “they provide the medium... they do not control the message.”<sup>28</sup> The Court decided in favour of the intermediaries, reasoning that if “an Internet intermediary does not itself engage in acts that relate to the content of the communication... but confines itself to providing ‘a conduit’ for information communicated by others” then it will not be deemed to be a participant to the infringement.<sup>29</sup>

The question, then, is when does an Internet intermediary cease to be “a conduit” and begin to be an active infringer? Justice Binnie explains that “notice of infringing content, and a failure to respond by ‘taking it down’ may in some circumstances lead to a finding of ‘authorization.’”<sup>30</sup> This uncertainty as to when authorization, and hence intermediary liability, occurs will surely cause intermediaries to err on the side of caution; upon the receipt of any notice, fear of legal consequences would cause intermediaries to take down content before they have the ability to consider whether or not the take down request is legitimate.<sup>31</sup> The practical effect for Internet intermediaries is that they will do their best to remain ignorant of their customers’ online gambling activities in order to avoid potential liability. Once they discover any questionable activity they will either (a) take down the website they are hosting, lose business, and face the possibility of a lawsuit from their hosting client; or (b) do nothing and face potential criminal legal responsibility. For Internet intermediaries, ignorance is bliss.

### **Where is the Line?**

From passive hosting to active promotion, there are varying degrees to which an

Internet intermediary might be involved with online gambling. Despite the dearth of legislation and case law dealing with Internet intermediary liability in the online gambling context, from the case law discussed above we can infer that (a) supplying the infrastructure for online gambling, such as passively hosting a website, will likely not constitute participation in illegal activity; and (b) to an extent, any implicit authorization does not constitute authorization to undertake illegal activity. This is all good news from the perspective of Internet intermediaries.

Attempting to infer the law of Internet intermediary liability in the online gambling context from cases discussing copyright infringement and the limited foreign jurisprudence available, however, can only provide a limited degree of insight and legal certainty. Passive or implicit authorization might involve inaction where action would have been required to stop the infringement, while active authorization might involve

express approvals or urgings to commit the act of infringement. There is a grey area in the middle of this spectrum in which it is difficult to demarcate between passive and active authorization; it is knowledge that transforms a passive conduit into an active—and potentially liable—participant. Because of the lack of case law in the online gambling context, it is difficult to be specific about what constitutes knowledge. Justice Binnie’s comments in *SOCAN* suggest that notice “may in some circumstances” amount to knowledge. Certainly, according to this logic it would be unacceptable in Canada for a telecommunications provider to actively partner with a purveyor of online gambling products as T-Mobile recently did with *Cecure Gaming*.<sup>33</sup> Enacting legislation, as the US did, or producing case law, as the UK did, that properly immunizes intermediaries would be helpful. Contrary to the age-old adage in business of “know your customer,” as it stands, legal uncertainty causes Internet

intermediaries to ensure they are as ignorant as possible of their customers’ identities and activities. Which leads us to the question, how can Canada foster a leading information technology industry when intermediaries cannot know their customers, implement effective business practices, or provide responsive customer service? **CGL**

*Both C. Ian Kyer and Andrew Alleyne of Fasken Martineau DuMoulin LLP act for a variety of clients in the online gaming industry. Ian Kyer is a senior partner practising corporate/commercial law with an emphasis on serving buyers and sellers of technology and related services. He is on the national steering committee of the firm’s Technology and Intellectual Property practice group. Andrew Alleyne is an associate practising corporate/commercial law with an emphasis on acquisitions, licensing, outsourcing and technology-related transactions.*

<sup>1</sup>[2004] S.C.J. No. 44 at 41 (*SOCAN*).

<sup>2</sup>*Ibid.*, see generally *Criminal Code*, R.S.C. 1985, c. C-46, ss. 202(1), (2), and 207 [Code]. See also C. Ian Kyer and Danielle Hough, “Is Internet Gaming Legal in Canada: A Look at Starnet” *Canadian Journal of Law and Technology*, Vol. 1 No. 1, online: [http://cjltd.dal.ca/vol1\\_no1/articles/01\\_01\\_KyeHou\\_gaming.pdf](http://cjltd.dal.ca/vol1_no1/articles/01_01_KyeHou_gaming.pdf) [Kyer & Hough “A Look at Starnet”] for an overview of the Code provisions that relate to online gambling.

<sup>3</sup>In the criminal stock fraud case of *Libman v. The Queen*, [1985] 2 S.C.R. 178 at 208 [Libman], where American purchasers were duped by a telephone call from Toronto and their money was routed through South America back to Canada, Justice La Forest explained on behalf of the Supreme Court, at 208, that it was appropriate for Canada to assume jurisdiction as “the transaction... is both here and there.” Justice La Forest, at 212-213, as cited in *SOCAN*, supra note 1 at 58, articulated the general principle regarding jurisdiction: “all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a ‘real and substantial link.’” Courts and tribunals have also applied what has come to be known as “the real and substantial connection” test (see *Morguard Investments Ltd. v. De Savoye*, [1990] 3 S.C.R. 1077 [Morguard]; *Beals v. Saldanha*, [2003] 3 S.C.R. 416) to defamation cases involving the cross-border dissemination of hateful information. For example, in *Citron v. Zundel*, (2002), 41 C.H.R.R. D/272, even though the host server was located in California, because the content provider and some of his audience was located in Canada, the Canadian Human Rights Tribunal assumed jurisdiction. Though not persuasive in Canada, see also the Australian case of *Dow Jones & Co. v. Gutnick* (2002), 194 A.L.R. 433, [2002] HCA 56 in *SOCAN*, supra note 1 at 41.

<sup>4</sup>*Morguard*, supra note 3.

<sup>5</sup>*Liberty Net*, *ibid.*; see also *WIC Premium Television Ltd. v. General Instrument Corp.* (2000), 8 C.P.R. (4th) 1 (Alta. C.A.); *Re World Stock Exchange* (2000), 9 A.S.C.S. 658 as cited in *SOCAN*, supra note 1 at 62.

<sup>6</sup>*Libman*, supra note 3.

<sup>7</sup>See *National Football League v. PrimeTime 24 Joint Venture*, 211 F.3d 10 (2d Cir. 2000) as cited in *SOCAN*, supra note 1 at 70.

<sup>8</sup>See *Los Angeles News Service v. Comus Communications Co.*, 969 F.Supp. 579 (C.D. Cal. 1997) as cited in *SOCAN*, supra note 1 at 71.

<sup>9</sup>See *Kyer & Hough “A Look at Starnet,” supra note 2.*

<sup>10</sup>See *SOCAN*, supra note 1 at 4.

<sup>11</sup>See *Re B.C. Motor Vehicle Act*, [1985] 2 S.C.R. 486; see generally s. 7 of the *Charter of Rights and Freedoms, of the Constitution Act, 1982*, enacted as *Schedule B to the Canada Act 1982 (U.K.) 1982*, c. 11: “Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.”

<sup>12</sup>See e.g. s. 202(2) of the Code, supra note 2: “every one who commits an offence under this section is guilty of an indictable offence and liable (a) for a first offence, to imprisonment for not more than two years; (b) for a second offence, to imprisonment for not more than two years and not less than fourteen days; and (c) for each subsequent offence, to imprisonment for not more than two years and not less than three months.”

<sup>13</sup>The official title is *Telecommunications Act of 1996*, Pub. L.A. No. 104-104, 110 Stat. 56 (1996).

<sup>14</sup>Title VIII of the *Security and Accountability For Every Port Act of 2006* (or *SAFE Port Act*, Pub.L. 109-347).

<sup>15</sup>*Bunt v. Tilley* [2006] EWHC 407 (QB).

<sup>16</sup>*Ibid.* at 36.

<sup>17</sup>*Ibid.* at 21.

<sup>18</sup>See *Falcon v. Famous Players Film Co.*, [1926] 2 KB 474. Similarly, in *Vigneux v. Canadian Performing Right Society, Ltd.*, [1945] A.C. 108 (P.C.) [Vigneux] the Privy Council held the defendant should not be held liable for authorizing the public performance of a phonograph as the record player was merely supplied by the defendant to a restaurant, and they had no control over its use. This position was largely adopted by the Supreme Court of Canada in *Muzak Corp. v. Composers, Authors and Publishers Association of Canada, Ltd.* [1953] 2 S.C.R. 182, where it was held that “something more” than the mere supply of the equipment required to infringe is needed to find the intermediary responsible.

<sup>19</sup>*De. Tervagne v. Beloeil (Town)* [1993], 3 F.C. 227 (F.C.T.D.); see also *R v. M. (J.P.)* 67 C.P.R. (3d) 152.

<sup>20</sup>*Copyright Act* (R.S., 1985, c. C-42), s. 3(1) [Copyright Act].

<sup>21</sup>[2004] 1 S.C.R. 339, 2004 SCC 13.

<sup>22</sup>*Ibid.* at 38.

<sup>23</sup>*Ibid.*

<sup>24</sup>*Electric Despatch Co. of Toronto v. Bell Telephone Co. of Canada* (1891), 20 S.C.R. 83, at p. 91 as cited in *SOCAN*, supra note 1 at 96.

<sup>25</sup>*Ibid.* per Justice Gwynne.

<sup>26</sup>*SOCAN*, supra note 1.

<sup>27</sup>Specifically, they argued that the “caching” process whereby the ISPs store recently searched websites to speed up later searches amounted to more than mere passive participation.

<sup>28</sup>*Ibid.* at 4.

<sup>29</sup>*SOCAN*, supra note 1 at 92. The Court focussed on the 1988 addition to the Copyright Act which suggests that intermediaries providing communication infrastructure are not considered parties to an infringing communication. See s. 2.4(1) of the Copyright Act, supra note 20: “For the purposes of communication to the public by telecommunication, ... (b) a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public.”

<sup>30</sup>*Ibid.* at 127 [emphasis added].

<sup>31</sup>At *ibid.* Justice Binnie recognizes this problem, explaining that “[a]n 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.”

<sup>32</sup>*Ibid.*

<sup>33</sup>T-Mobile recently partnered with *Cecure Gaming*, to allow users to download *Cecure Gaming* applications, such as the poker game *Aces Royal*, from the cash games section of T-Mobile’s games portal, onto their mobile device without having to go into the open internet. See Alex Wade, “Offshore Operator Steps Up To UK’s Software Rules” [gamblingcompliance.com](http://gamblingcompliance.com), 11 June 2007.