Focus

INFORMATION TECHNOLOGY

YMGERMAN / ISTOCKPHOTO.COM

Bending the law for more Netflix

Virtual private network users ignore geographic boundaries to occupy legal grey area

Jordan Walbesser

As an engineer-turned-attorney, it's unsurprising that I rely on various gizmos and gadgets for news and communication. Recently, with services like Netflix, I get my entertainment fix through online streaming — so do a third of Anglophone Canadians, according to a recent Media Technology Monitor study. But not all streaming media experiences are made equal.

Like many of us, I often travel between the United States and Canada. And like many of you, I noticed that Netflix's offerings change based on my location. Netflix performs this technological feat based on my device's IP address. IP addresses are the electronic code that lets a server know which device on the Internet is which. It just so happens that IP addresses are assigned geographically.

When it comes to Netflix, location makes a big difference. It turns out that a U.S. viewer can select from over 10,000 titles in comparison to a Canadian viewer's 4,000. This disparity is a result of the prevailing content owners' business model — called "windowing."

Content owners intentionally license media in "windows" to increase sales and maximize profit. For example, in order to boost repeat sales, movies start in theatres, and then sequentially release on other platforms like DVD, TV, iTunes and Netflix. Through licensing, content owners also enforce geographical windows. Windowing is a profitable model for content owners, but limiting access to content is inconvenient for consumers. For Netflix, that inconvenience helps explain why 35 per cent of Canadian users mask their location to access the U.S. Netflix library.

Masking your location online has become user-friendly through the proliferation of inexpensive virtual private networks (VPNs). A VPN creates a secure "tunnel" between your device and a server which may reside in a different country. All requests to the Internet flow through the server, and the server brings the results back to your device. Generally, VPNs are legal in Canada and the United States. However, the legality of using a VPN to make Netflix think your device is elsewhere remains a grey area.

Using a VPN to trick Netflix clearly violates Netflix's terms of use. For Canadians and Americans, the Netflix terms of use is governed under U.S. law, including the much-maligned — and outdated — *Computer Fraud and Abuse Act* (CFAA).

Previously, some U.S. website owners invoked the CFAA to enforce website terms of use, arguing that a website user "exceeds authorized access" by accessing a site in violation of its terms of use. However, the Northern District of California held that a defendant was not liable under the CFAA for simply violating the terms of use. Instead, a defendant could only face CFAA liability if they circumvented "technical barriers" such that the access itself was not authorized.

But does a VPN circumvent technical barriers? In August 2013, a U.S. District

Windowing, Page 15

This article originally appeared in the October 3, 2014, issue of *The Lawyers Weekly* published by LexisNexis Canada Inc.

Focus INFORMATION TECHNOLOGY

‘Notice and Notice’ coming for online copyright


John Cotter
Martin Brandsma

Copyright owners have always been free to notify online mediators of alleged copyright infringement, but until now there has been no legislation dealing with such notices. The new sections 41.25, 41.26 and 41.27(3) of Canada’s *Copyright Act*, dubbed the “Notice and Notice” regime, deal with such notices and these sections come into force on Jan. 2. The amendments are the last changes to *The Copyright Modernization Act* and are the last to come into force — the majority became law in November 2012. The government describes the regime as a “made-in-Canada” solution to combat copyright infringement in the “modern digital age.”

The new legislation targets two broad categories of entities, each engaged with facilitating access to online materials:

- Internet-service providers (i.e., persons providing services related to the operation of the Internet or another digital network) and website hosts (i.e., persons providing digital memory in which another person stores a work or other subject matter); and
- Search-engine providers (i.e., persons who provide an information location tool, which is defined as any tool that makes it possible to locate information that is available through the Internet or another digital network).

The obligations on these two groups are triggered under the new sections once notice of alleged infringement is received from a copyright owner. For the notice to be effective, it must contain the information that is prescribed in the *Copyright Act* (see ss. 41.25(2)). This includes such things as the “location data for the electronic location to which the claimed infringement relates” and “the date and time of the commission of the claimed infringement.” Assuming that the notice meets these requirements, the consequences of the notice depend on whether the recipient is an ISP or website host on the one hand, or a search-engine provider on the other.

KIKKERDIRK/ ISTOCKPHOTO.COM

> The legislation does not require ISPs or website hosts to take down allegedly infringing material, as is the case in the comparable U.S. legislation... This may leave open the question of whether an ISP or website host that does not comply with demands made by copyright owners to remove infringing works are potentially liable for copyright infringement...
>
> **John Cotter and Martin Brandsma**
> Osler, Hoskin & Harcourt

ISPs and website hosts

The new sections require all ISPs or website hosts receiving proper notice to forward the notice electronically “as soon as feasible” to the customer associated with the allegedly infringing activity (new ss. 41.26(1)(*a*)). The section does not use the term customer; it provides that the notice is to be forwarded to “the person to whom the electronic location identified by the location data specified in the notice belongs.” ISPs and website hosts must also inform the copyright owner once they have forwarded the notice (or the reason why it was not possible to do so) and “retain records that will allow the identity of the person to whom the electronic location belongs to be determined” (new ss. 41.26(1)(*b*)). These records must be maintained for six months from receipt of the notice, or twelve months if legal proceedings are commenced (provided that the ISP or website host received notice of the legal proceedings before the end of the initial six-month period). ISPs and website hosts are also not permitted to charge a fee for forwarding the notice (since regulations were not prescribed; see new ss. 41.26(1) and (2)).

ISPs or website hosts failing to forward a proper notice are subject to statutory damages of at least $5,000, but which are capped at $10,000 (new ss. 41.26(3)).

The legislation does not require ISPs or website hosts to *take down* allegedly infringing material, as is the case in the comparable U.S. legislation. Although the amendments do not impose such a requirement on ISPs or website hosts, the amendments do not specifically provide that there is no liability if the material is not taken down. This may leave open the question of whether an ISP or website host that does not comply with demands made by copyright owners to *remove* infringing works are potentially liable for copyright infringement (see, for example, *SOCAN v CAIP* [2004] S.C.J. No. 45, at para. 110, which, of course, was decided well before the notice and notice regime).

Search-engine providers

The starting point for a discussion of the consequences on search-engine providers is subsections 41.27(1) and (2), which provide that in proceedings for copyright infringement against a search-engine provider, the only remedy available is an injunction (provided that certain conditions are met). Unlike the situation for both ISPs and website hosts, search-engine providers are not obligated to forward notices they receive. However, where a notice has been sent to a search-engine provider and the allegedly infringing material has already been removed, the search-engine provider loses the benefit of subsection 41.27(1) for reproductions made more than 30 days after receipt of the notice (new ss. 41.27(3)). In other words, a search-engine provider has 30 days to remove cache copies, after which time they may be liable for damages for copyright infringement.

There will be a number of interesting questions the courts will need to consider once copyright owners begin to rely on these new provisions, and the extent of their impact may not be known until there is some judicial consideration of them.

John Cotter is an IP/IT litigator and a partner, and Martin Brandsma is an IP litigator and associate with Osler, Hoskin & Harcourt.

Windowing: Hulu has banned subscribers for unauthorized access

Continued from page 14

Court Judge ruled that using a VPN to circumvent a blocked IP address was indeed a breach of the CFAA. However, in this case, the perpetrator’s IP address was previously blocked due to his previous intrusions to access private data. The perpetrator used a VPN to mask his location through a new IP address. Consequently, this case is distinguishable from a Netflix VPN because Netflix is available to the user without use of the VPN.

In Canada, the *Copyright Act* and the *Digital Privacy Act* govern how users access copyrighted media content. Changes to both acts may require that Internet service providers share customer data with any organization (private or public) that investigates a contractual breach. In other words, a VPN or an ISP could be forced to provide a customer list of VPN users. These users might run the risk of prosecution under the *Copyright Act* if the VPN is used to access unlicensed content in Canada. At present, however, since the content is not licensed for use in their actual locale, Netflix and the content providers seem unwilling to interfere with VPN-armed users.

In fact, Netflix is aware of VPN usage. Netflix spokesperson Jenny McCabe said “We know it goes on. We don’t condone it.” But so far, Netflix has not banned subscribers for using VPNs (Netflix’s chief competitor, Hulu, has done so). Unless Netflix begins enforcing its terms of use, or content providers begin to pressure Netflix to do so, the use of VPNs to access geographically-limited content will likely continue.

Netflix seems content to apply pressure on traditional licensing models by producing original content and releasing it the way we like it: all at once, and everywhere.

“We believe that when you provide great content to people and you make it available, they choose the legal route,” says Netflix spokesperson Jenny McCabe. “What prevents people from being able to watch what they want are the classic windowing systems that exist in the content world.”

Until windowing becomes obsolete, users will have to navigate the legal grey area or otherwise miss out on geographically-limited content.

Jordan Walbesser, a lawyer at Hodgson Russ, concentrates his practice in intellectual property law, with a focus on patents and business methods. He is also well versed in software, cloud computing, social media, and peer-to-peer networking issues.