VOLUME 22 SUMMER 2017

ILLINOIS BUSINESS LAW JOURNAL

EQUATING CYBERTRAVEL WITH PHYSICAL TRAVEL: THE KEY TO PRESERVING A BORDERLESS INTERNET WITHOUT VIOLATING U.S. COPYRIGHT LAW

❖ NOTE ❖

*Michal Nowicki**

TABLE OF CONTENTS

I. INTRODUCTION

"We're sorry, this content is not available outside of Canada. If you believe you received this message in error please contact us."[1] The above text is an example of an error message displayed when Internet users try to access geographically restricted web content from outside the authorized viewing territory. Website operators restrict access to digital content geographically for several reasons, including to promote targeted advertising, to comply with local

[1] CBC TV, http://watch.cbc.ca/shows/ (last visited May 22, 2017).

*J.D. Candidate, Class of 2018, University of Illinois College of Law.

laws and regulations, to prevent financial fraud, and, in the case of online streaming services like Netflix, to protect the intellectual property rights of content licensors.[2] Not surprisingly, Internet users frequently bypass these restrictions by employing a variety of methods designed to trick websites into thinking that the user is accessing them from a different country or region. Since governments do not yet specifically regulate the circumvention of geoblocks, its use has become a legal grey area,[3] particularly where its purpose is to gain access to copyright-restricted content.

This Note examines the legality of cybertravel—the use of technological measures to trick a website into believing that the user is accessing it from a different location—for the sole purpose of accessing copyright-restricted web content not offered in the user's physical location. In so doing, it focuses exclusively on the circumventor's direct liability under the Digital Millennium Copyright Act (DMCA).[4] Concluding that such geo-dodging violates § 1201, it urges courts to exempt cybertravel from the DMCA by equating it with physical travel. Part II provides background information on geolocation tools and the techniques used to circumvent them. Part III discusses the DMCA and explains why its plain language supports extending it to cybertravel. Part IV recommends that courts not apply the DMCA to cybertravel because cybertravel is analogous to physical travel in all material respects, and the right to travel internationally is implicitly protected by the Fifth Amendment to the United States Constitution. This Note argues that while the ordinary meaning of § 1201 of the DMCA supports extending it to copyright-evading cybertravel, the DMCA should not apply to cybertravel because an Internet traveler should be treated the same as a physical traveler, meaning that the law of his or her virtual location should apply to any geolocation evasion activity.

II. BACKGROUND

A. Geoblocking and Geolocation Tools

---

[2] *See generally* Marketa Trimble, The *Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 586–90 (2012) (discussing these and other uses of geolocation).

[3] Michelle Edelman, *The Thrill of Anticipation: Why the Circumvention of Geoblocks Should be Illegal*, 15 VA. SPORTS & ENT. L.J. 110, 111 (2015).

[4] 17 U.S.C. § 1201 (2012). This Note does not address other, less controversial uses of cybertravel, such as to display advertisements from another region, or to access mobile or online banking from outside the user's home country, nor does it analyze potential third-party liability for any copyright infringement.

Geoblocking is defined as "limiting the user's access to digital content, by the content distributor, based on the user's geographical location."[5] It functions as "an extension of digital rights management (DRM) that enables a copyright holder to control access to his work and control the release of content."[6] Traditional geolocation methods can be divided into three categories: self-reporting, Internet Protocol (IP) geolocation, and timing and distance-based techniques.[7] As its name suggests, the self-reporting method asks the user to "report" their location.[8] Examples of self-reporting mechanisms include location fields in an online registration form and dropdown menus listing countries which, when activated, take the user to the country-specific page of a website based on the user's selection.[9] While self-reporting is sufficient for tailoring advertising or "facilitating convenient content" (e.g., pricing in local currency), it is inadequate for enforcement because users can easily misrepresent their location by choosing an option that does not correspond to their physical location.[10] Moreover, if the website relies on cookies stored on the user's computer to track the user's location, the computer's future relocation will not update the reported location information.[11] Consequently, self-reporting tools are rarely used to prevent copyright infringement.[12]

By contrast, IP geolocation is used most frequently to enforce copyright holders' territorial rights.[13] IP addresses are "numeric strings tied to a computer or other device accessing the Internet."[14] They are analogous to physical mailing addresses in that "they allow for accurate transmittal and receipt of data."[15] When a device accesses the Internet, it announces its IP address, thereby allowing others to geolocate it.[16]

Like self-reporting mechanisms, IP geolocation is presently incapable of pinpointing the user's precise physical location. Nevertheless, it can normally

---

[5] Tal Kra-Oz, *Geoblocking and the Legality of Circumvention*, 57 IDEA: J. FRANKLIN PIERCE FOR INTELL. PROP. 385, 388 (2017).
[6] Edelman, *supra* note 3, at 112.
[7] Jerusha Burnett, *Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules*, 19 MICH. TELECOMM. & TECH. L. REV. 461, 465 (2012).
[8] *Id.*
[9] Trimble, *supra* note 2, at 592–93.
[10] Burnett, *supra* note 7, at 466; Trimble, *supra* note 2, at 593.
[11] Burnett, *supra* note 7, at 466.
[12] *See id.*
[13] Kra-Oz, *supra* note 5, at 389.
[14] Burnett, *supra* note 7, at 466.
[15] Trimble, *supra* note 2, at 594.
[16] *Id.* at 596.

provide a "ballpark estimation of the user's location."[17] This identification of the user's approximate location is sufficient for copyright enforcement because most geoblocked content is not further restricted within national borders.[18]

There are two basic types of time-based geolocation tools. First, a website operator can use code to request time of day, which will, at a minimum, give it the user's computer's time zone.[19] Alternatively, a website operator can measure the time necessary to receive a reply from the host or study the path taken to reach the host.[20] Finally, with the advent of smartphones, and the resulting emergence of mobile apps, some streaming services now geolocate subscribers using the GPS receivers built into their mobile devices.[21]

Website operators create virtual borders for several reasons.[22] In the video streaming context, they do so because their license agreements with copyright holders, such as film studios and television stations, require them to protect the copyright holders' exclusive right to control access to copyrighted content. [23] For example, under U.S. copyright law, the copyright holder has the exclusive right, subject to several exceptions, to "reproduce," "prepare derivative works based upon," "distribute," and to "perform "and "display" publicly," the copyrighted work.[24] Section 1201 of the DMCA, discussed in Part III, enforces this right.

B. Geolocation Evasion Tools

Internet users employ various methods to circumvent IP-based geoblocks. Trimble divides these methods into two categories: "self-sustained" and mainstream.[25] Self-sustained solutions are so named because they facilitate cybertravel through equipment owned by the user directly, or by the user's

---

[17] Kra-Oz, *supra* note 5, at 389.
[18] *Id.*
[19] Burnett, *supra* note 7, at 468.
[20] *Id.* at 469.
[21] *See* Kra-Oz, *supra* note 5, at 388–89.
[22] *See supra* note 2 and accompanying text.
[23] *See* Edelman, *supra* note 3, at 110 (noting that "[m]edia companies, and film studios in particular in the U.S., make a large part of their profits on a timed-window release system: movies come out in theatres before they are available to rent, before they are available to stream. This timed release includes a geographic component: movies (theatrical, home video, or streaming) are made available in some countries before others to allow for the effectiveness of ad campaigns, to tailor to the specific tastes of different markets, and to license content by territory.")
[24] 17 U.S.C. § 106 (2012).
[25] Trimble, *supra* note 2, at 600–01.

friends or relatives in a foreign country.[26] As Trimble explains, these tools enable an Internet user to access remotely a computer located anywhere in the world, thereby taking advantage of its Internet connection and foreign IP address.[27] Mainstream tools include dial-up connections to internet service providers in foreign countries,[28] software and web-based proxy servers,[29] virtual private networks (VPNs) (some of which specialize in cybertravel to specific countries),[30] and Domain Name Service (DNS) proxy services like Unblock-US, which are designed to unblock specific websites.[31] Although each geolocation tool operates differently, all of the above-mentioned tools make it appear as though the user is accessing geoblocked content from within the authorized territory by rerouting the user's Internet connection through a server in that territory.

III. ANALYSIS

The DMCA outlaws the circumvention of technological measures used to prevent unauthorized access to copyrighted material. It provides, in pertinent part, "No person shall circumvent a technological measure that effectively controls access to a work protected under [U.S. copyright law]."[32] The DMCA defines circumvention of a technological measure as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[33] While one could otherwise argue that § 1201(a)(1)(A) does not cover cybertravel to evade copyright-motivated geoblocking because currently-used geolocation tools do not "*effectively* control access" to copyrighted works, given that it is "fantastically easy" to thwart geolocation tools,[34] the statute clarifies that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the

[26] *Id.* at 601.
[27] *Id.* at 600–01.
[28] *Id.* at 601.
[29] *Id.* at 602.
[30] *Id.* at 603.
[31] Edelman, *supra* note 3, at 115.
[32] 17 U.S.C. § 1201(a)(1)(A) (2012).
[33] 17 U.S.C. § 1201(a)(3)(A) (2012).
[34] Trimble, *supra* note 2, at 599.

work."[35] Consequently, the DMCA very likely covers copyright-infringing cybertravel.

A. Plain Language of the DMCA

Although there is no judicial precedent in the United States as to whether the DMCA's direct anticircumvention provision encompasses copyright-infringing cybertravel,[36] a court would very likely conclude that it does, based on the plain language of § 1201(a)(1)(A). As Edelman correctly observes, geoblocking satisfies the statutory definition of a "technological measure" because "the detection of the location of the IP address of someone trying to gain access to a streaming provider is an 'application of information' that allows a streaming provider to control access to the work of the copyright holder."[37] More specifically, geoblocking constitutes a "technological measure" protecting the copyright holder's exclusive right to "distribute" copies of the copyrighted content to the public under 17 U.S.C. § 106.[38] Moreover, as explained above, the argument that geoblocking does not "effectively" control access to the restricted content because geolocation evasion tools are ubiquitous is unconvincing due to the low statutory "effective control" threshold.[39] Finally, the circumvention element is satisfied most easily, as DNS proxy services like Unblock-US not only offer the ability to "bypass" geoblocks, but are designed precisely and exclusively for that purpose.[40] Thus, if a U.S. court were to apply § 1201(a)(1)(A) of the DMCA, it would very likely conclude that it covers copyright-infringing cybertravel.

B. Exceptions to § 1201(a)(1)(A)

Although § 1201(a)(1)(A) is subject to several exceptions, none of them likely applies to copyright-infringing cybertravel. For instance, while the statute empowers the Librarian of Congress to exempt specific circumvention

---

[35] 17 U.S.C. § 1201(a)(3)(B) (2012); *see also* 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004) (rejecting the argument that a technological measure cannot be considered effective if its countermeasures are 'widely available on the Internet').

[36] Edelman, *supra* note 3, at 116. The only on-point case, *TVB Holdings, Inc. v. Tai Lake Commc'ns*, No. CV12-09809, 2013 WL 6417330 (C.D. Cal. Oct. 1, 2013), settled prior to judgment on the merits. Edelman, *supra* note 3, at 116 n.36.

[37] *Id.* at 118.

[38] *Id.*

[39] *See supra* note 35 and accompanying text.

[40] *Id.* at 119.

activities that "adversely affect," or will likely "adversely affect" within the next three years, a user's ability to "make noninfringing uses" of the types of copyrighted works in question,[41] none of the exemptions currently in force address cybertravel; most, though not all, relate to compatibility with assistive technology used by the disabled, or to software interoperability.[42] Other statutory exceptions, such as the exemptions for "nonprofit libraries, archives and educational institutions,"[43] "law enforcement, intelligence, and other government activities,"[44] interoperability-driven "reverse engineering,"[45] permitted "encryption research,"[46] and "permissible acts of security testing"[47] are much narrower and fall even farther outside the scope of geolocation evasion.

The only statutory exception that could potentially shield geolocation evaders from direct liability for copyright infringement under the DMCA relates to the protection of "personally identifying information" (PII) but even that exception is highly problematic.[48] Under this exception:

> Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—
>
> (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;
>
> (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

---

[41] 17 U.S.C. § 1201(1)(B)–(C) (2012).
[42] Burnett, *supra* note 7, at 476.
[43] 17 U.S.C. § 1201(d) (2012).
[44] 17 U.S.C. § 1201(e) (2012).
[45] 17 U.S.C. § 1201(f) (2012).
[46] 17 U.S.C. § 1201(g) (2012).
[47] 17 U.S.C. § 1201(j) (2012).
[48] 17 U.S.C. § 1201(i) (2012).

> (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and
>
> (D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.[49]

The "and" at the end of subparagraph (C) indicates that all four elements must be satisfied to successfully invoke the PII exception. The Federal Trade Commission has traditionally defined PII as "information that can be linked to a specific individual including, but not limited to, name, postal address, email address, Social Security Number, or driver's license number."[50] While Jerusha Burnett acknowledges that not all geolocation tools are sufficiently precise to facilitate the collection of PII,[51] she argues that since most websites collect other information about their visitors in addition to their location, the "aggregated" data may "suffic[e] to identify an individual."[52]

While Burnett's conclusion may be correct, it is ineffective for protecting an Internet user's right to travel in cyberspace for several reasons. First, it is unclear whether courts may consider data in the "aggregate" in determining whether such data suffices to identify an individual, or whether the user's IP address must be capable of doing so alone. If the latter is true, Internet users who wish to stream geoblocked content unavailable in their country will not be able to rely on the PII exception because while IP geolocation tools are accurate enough to enforce national and even regional geoblocks,[53] they are too imprecise to reveal the user's identity. This is especially true if the user accesses the websites from a shared network, whether it be from a private computer used by other members of their household, or from a public device at work, in a library, or at an Internet café. Therefore, while some geolocation tools may allow a website operator to discover the user's identity by tracing their IP address to their Internet Service Provider, thereby satisfying subparagraph (A), many streaming services, especially ones available for free and without

---

[49] 17 U.S.C. § 1201(i)(1) (2012).
[50] Burnett, *supra* note 7, at 482.
[51] *Id.* at 482–83.
[52] *Id.* at 483.
[53] *See supra* notes 19–20 and accompanying text.

registration in the authorized viewing territory, might not actually collect PII, in which case subparagraph (B) is not met. Most important, though, even if a website operator can collect PII and in fact does so, it can easily defeat future § 1201(i) claims by providing clear notice to its visitors that it gathers their personal information.

IV. RECOMMENDATION

Since § 1201(a)(1)(A) of the DMCA very likely prohibits international cybertravel to access services like Netflix, and since none of its exceptions offer a reliable escape route, the key to preserving a borderless Internet is to take geolocation evasion outside the DMCA by treating cybertravel the same as physical travel: at least for copyright infringement liability purposes.[54] Under this approach, the cybertraveler would be subject to the law of their virtual location with regards to their online activity while using a geolocation evasion tool, just as a physical traveler is subject to the criminal law of the jurisdiction where he or she commits a crime. Thus, for example, a German resident accessing the U.S. version of Netflix from Germany via a VPN or DNS proxy could not be held liable for direct copyright infringement under the DMCA because he would be deemed within U.S. borders at the time of the act, where access to U.S. Netflix is lawful.

Although courts might be reluctant to adopt such a radical approach because it ignores the intellectual property interests of copyright holders, the argument for equating cybertravel with physical travel has constitutional and international support. In *Kent v. Dulles*, the Court recognized an implied constitutional right to travel internationally.[55] There, the plaintiffs' request for a U.S. passport was denied because of their affiliation with the Communist Party.[56] Without ruling on the constitutionality of the applicable regulation, the Court held that "The right to travel is a part of the 'liberty' of which the citizen cannot be deprived without the due process of law under the Fifth Amendment."[57] In doing so, it explained:

> Freedom of movement across frontiers in either direction, and inside frontiers as well, was a part of our heritage. Travel abroad, like travel within the country, may be necessary for a

---

[54] *Cf.* Trimble, *supra* note 2 at 572 (limiting this argument to cybertravel for non-infringing reasons). Trimble does not, however, advocate for treating all forms of cybertravel the same as physical travel.
[55] 357 U.S. 116, 125 (1958).
[56] *Id.* at 117–20.
[57] *Id.* at 125.

> livelihood. It may be as close to the heart of the individual as the choice of what he eats, or wears, or reads. Freedom of movement is basic in our scheme of values. . . . Freedom of movement also has large social values. Foreign correspondents and lecturers on public affairs need first-hand information. Scientists and scholars gain greatly from consultations with colleagues in other countries. Students equip themselves for more fruitful careers in the United States by instruction in foreign universities. Then there are reasons close to the core of personal life—marriage, reuniting families, spending hours with old friends.[58]

Although some of the values associated with freedom of movement cited in *Kent* are irrelevant to cybertravel, others, such as unique business and educational opportunities, apply to cybertravel and physical travel alike.[59] For example, under European Union (EU) law, a member state may not refuse to register, within its borders, a branch office of a company formed under the laws of another member state, solely because it finds that the branch office structure intends to escape unfavorable national laws.[60] In *Centros*, two Danish citizens living in Denmark wanted to set up a private limited liability company in Denmark.[61] However, Danish law required a minimum capital investment of DKK 200,000 — the equivalent of approximately $30,000 — to form a new private limited company.[62] To avoid this obstacle, the partners registered their business in the United Kingdom, which had no minimum capital requirement.[63] They then applied for a branch office in Denmark.[64] The company did no business in the UK,[65] and a friend of the owners agreed that his home would constitute the company's registered office in the UK.[66] The Danish Trade and Companies Board rejected the company's application for a branch office because it concluded that its owners sought to circumvent Danish law by establishing a principal office, not a branch, in Denmark.[67] The

---

[58] *Id.* at 126–27.
[59] Trimble, *supra* note 2, at 641.
[60] Case C-212/97, Centros Ltd. V. Erhvervs-og Selskabsstyrelsen, 1999 E.C.R. I-01459, ¶ 30.
[61] *Id.* ¶ 2.
[62] *Id.* ¶ 7.
[63] *Id.* ¶ 3.
[64] *Id.* ¶ 6.
[65] *Id. ¶ 7.*
[66] *Id.* ¶ 3.
[67] *Id.* ¶ 7.

company subsequently sued the Board under EU law to compel it to register a Danish branch office. The European Court of Justice (ECJ) held that "[T]he fact that a company does not conduct any business in the Member State in which it has its registered office and pursues its activities only in the Member State where its branch is established is not sufficient to prove the existence of abuse or fraudulent conduct which would entitle the latter Member State to deny that company the benefit of the provisions of Community law relating to the right of establishment" guaranteed by Articles 52 and 58 of the Treaty on the Formation of the European Union.[68] The court importantly clarified that "it is immaterial that the company was formed in the first Member State only for the purpose of establishing itself in the second, where its main, or indeed entire, business is to be conducted."[69]

Although EU cases do not bind American courts, the ECJ's decision in *Centros* rests on the same broad legal grounds as *Kent, and both cases support equating cybertravel with physical travel.* While the two cases have been decided under the laws of two fundamentally different legal systems, both *Kent* and *Centros* recognize freedom of movement across borders as an inalienable right. Specifically, *Kent* does so in the context of international travel, whereas *Centros* accomplishes this in the context of international commerce. The fact that Denmark and the UK are both EU members does not defeat the analogy because even though both countries must comply with EU laws, they each still have their own national laws regulating domestic businesses, laws which control whenever they do not conflict with EU law.

Just as American and European entrepreneurs are free to register their businesses wherever they please, Internet users should be allowed to cybertravel so that streaming services and geolocation evasion services can continue to prosper. While there are no reliable estimates of how many streaming service subscribers use VPNs, restricting cybertravel would likely increase piracy,[70] because cybertravelers would no longer be able to access many of the territorially-restricted websites they visit today. As a result, the grey market for geolocation evasion we have now would likely turn into a black market for copyright-protected content. If governments allow such a black market to develop, it will become difficult, if not impossible, to eliminate it, since illegal activity is generally more difficult to monitor and control than semilegal conduct. Moreover, geolocation evasion services, especially DNS proxy providers like Unblock-US, would suffer or even go out of business. However,

---

[68] *Id.* ¶ 29.
[69] *Id.* ¶ 17.
[70] *See* Julia Greenberg, *For Netflix, Discontent Over Blocked VPNs is Boiling*, WIRED.COM (Mar. 7, 2016, 7:00 AM), https://www.wired.com/2016/03/netflix-discontent-blocked-vpns-boiling/ (warning that Netflix's crackdown on VPN usage may lead to piracy).

treating cybertravel the same as physical travel would prevent these problems because Internet users would be able to continue satisfying their thirst for entertainment through legitimate streaming services like Netflix, since they would have no need to resort to websites that have no right to broadcast the content to anyone. At the same time, VPN and proxy DNS providers would enjoy the same (if not greater) profits they make today.

Equating cybertravel with physical travel would also create new cultural and educational opportunities. First, bypassing Internet geoblocks allows emigrants to watch television shows from their native country not otherwise available for viewing in their new country, thereby enabling them to keep up with cultural changes in the same way they would if they physically visited that country. Likewise, an individual studying a foreign culture need not travel abroad to do so because he or she can gain valuable information from streaming documentaries, live events, and other geographically-restricted content from that country. In both situations, cybertravel is often preferable over physical travel because it is less costly and less time-consuming; VPN and DNS proxy subscribers pay a fraction of the price of a plane ticket, while rerouting one's Internet connection through a foreign server is instantaneous, compared with international physical travel, which lasts several hours.

Finally, equating cybertravel with physical travel would help restore a borderless Internet. As Trimble explains, the Internet was originally designed as a "decentralized network" without territorial boundaries.[71] The U.S. Department of Defense admired this design because "such an architecture was more likely to withstand an enemy attack."[72] Today, however, the Internet no longer functions as a borderless medium, in part due to widespread geoblocking worldwide. While making geolocation evasion easier or eliminating geoblocking altogether would not remove all territorial borders because governments regulate Internet usage in other ways, it would constitute a major step in that direction.

Restoring a borderless Internet would benefit cybertravelers in two important ways. First, it would promote free speech. Since cybertravelers would gain access to a global media market without fear that their favorite streaming service may someday block their VPN or proxy, they would be exposed to a wider variety of viewpoints. This increased exposure would give them opportunities to form new opinions, which they would be entitled to share with others. Second, since most geolocation evasion tools encrypt the user's Internet connection in addition to concealing their IP address, cybertravelers would enjoy greater privacy.

---

[71] Trimble, *supra* note 2, at 675.
[72] *Id.* at 676.

Although equating cybertravel with physical travel would harm copyright holders of geoblocked content, copyright holders could explore other avenues to offset their lost profits. For instance, instead of staggering releases, as many film studios do today, they could focus more on attractive advertising techniques to increase revenue. Additionally, the copyright owners of international live sporting events could appeal to their viewers' personal preferences. For instance, many Americans prefer foreign, English-language broadcasts of the Olympics over local coverage because NBC, the network with exclusive rights to stream the Olympics in the United States, constantly interrupts its broadcasts with commercials.[73] Content owners could take advantage of this flaw by advertising available commercial-free options. In both scenarios, content owners would relinquish the right to control access to their works, but their losses could be minimal, while consumers would have greater access to digital content.

V. CONCLUSION

While it remains "fantastically easy" to fake one's virtual location,[74] the future of cybertravel to access copyrighted, geoblocked content is questionable because of anticircumvention laws like the DMCA. The ordinary meaning of the DMCA supports extending the statute to geolocation evasion because geoblocking qualifies as a "technological measure" implemented to control access to a copyrighted work, because it meets the "effective control" statutory threshold, and because copyright-infringing cybertravel occurs precisely to circumvent geoblocking.[75] However, since U.S. courts have not yet had the opportunity to so construe the DMCA, cybertravelers seeking to stream geographically-restricted content from outside the authorized viewing area still have hope. To protect their interests, courts and legislatures should treat cybertravel the same as physical travel. As discussed above, this recommendation has legal support.[76] While this proposal may upset content

---

[73] *See* Harriet Alexander, *NBC Criticized for "Worst Ever" Olympic Coverage in America*, THE TELEGRAPH (Aug. 10, 2016, 11:47 PM), http://www.telegraph.co.uk/olympics/2016/08/10/nbc-criticised-for-worst-ever-olympic-coverage-in-america/ (noting that there were five commercial breaks in the first thirty minutes of NBC's broadcast of the 2016 Summer Olympics opening ceremony); JENNI RYALL, *The NBC Olympics Coverage Is a Total, Commercial-Filled Nightmare*, MASHABLE.COM (Aug. 5, 2016), http://mashable.com/2016/08/05/nbc-olympics-fail/#pFELV_T_umqJ (encouraging Americans to watch British or Australian coverage of the Olympics).

[74] *See supra* note 34 and accompanying text.

[75] *See supra* Part III.

[76] *See supra* Part IV.

owners because it limits their ability to control access to their works, the commercial, educational, and cultural benefits of allowing cybertravel outweigh any harm to copyright holders, since content owners can adapt by adjusting their advertising campaigns to take advantage of the additional business cybertravel could bring to them. Moreover, lawful cybertravel would constitute a major step towards reviving a borderless Internet. In light of these considerations, governments should encourage cybertravel.