NOTE

GEOGRAPHICALLY RESTRICTED STREAMING CONTENT AND EVASION OF GEOLOCATION: THE APPLICABILITY OF THE COPYRIGHT ANTICIRCUMVENTION RULES

*Jerusha Burnett**

Cite as: Jerusha Burnett, *Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules*, 19 MICH. TELECOMM. & TECH. L. REV. 461 (2012), available at http://www.mttlr.org/volnineteen/burnett.pdf

A number of methods currently exist or are being developed to determine where Internet users are located geographically when they access a particular webpage. Yet regardless of the precautions taken by website operators to limit the locations from which they allow access, it is likely that users will find ways to gain access to restricted content. Should the evasion of geolocation constitute circumvention of access controls so that § 1201 of the Digital Millennium Copyright Act ("DMCA") applies? Because location data can properly be considered personally identifiable information ("PII"), this Note argues that § 1201 should not apply absent a warning that such data is being collected by the website operator. One interpretation of the anticircumvention rules requires no violation of the rights granted to the copyright holder by 17 U.S.C. § 106. A better interpretation, however, would require some violation of those rights and would also allow the evasion of geolocation when streaming online content. This Note seeks to explore the existing legal framework within the technological context and to propose solutions which balance the needs of users against those of the website operators and copyright holders.

* J.D. University of Michigan Law School expected 2014; M.S.I. University of Michigan School of Information expected 2014. Thank you to the Volume 19 editorial staff, particularly Alexa Nickow, Liza Roe, and Mary Harmon for their excellent comments.

Introduction

Both seasons of the recently popular British television show *Sherlock* aired in the United Kingdom on the BBC several months before they aired in the United States on PBS.[1] The seasons aired in the U.S. in a slightly edited form; the unedited versions were unavailable to U.S. viewers until they were released on DVD and made accessible via streaming on sites such as Netflix. Not so long ago, waiting would have been the only option for the likely small number of viewers who even knew of the show's airing. The Internet has changed this simple fact. Now, any interested person can hear about the episode in minute detail as it airs even if they cannot watch it.[2] After *Sherlock*'s broadcasts in the U.K., the BBC made the full episodes available via streaming only for viewers located in the U.K. The first episode of season two even broke the record for total visits from Internet users purportedly in the U.K. the day after it originally aired.[3] It is possible, though not certain, that some of these viewers were located outside of the U.K. As will be discussed in Part I.C of this Note, it is relatively easy to convince any website

1. For example, episode one of season two first aired on BBC One in the U.K. on January 1, 2012, while the same episode first aired on PBS in the U.S. on May 6, 2012, a full four months later. *BBC One – Sherlock – Episode Guide*, BBC, http://www.bbc.co.uk/programmes/b018ttws/episodes/guide#p00m5wm7 (last visited Dec. 29, 2012); *Sherlock*, Masterpiece, http://www.pbs.org/wgbh/masterpiece/sherlock/ (last visited Dec. 29, 2012).

2. *See, e.g.*, Brian Mansfield, *'American Idol' Baton Rouge: the Live Blog*, USA Today (Jan. 24, 2013, 9:28 PM), http://www.usatoday.com/story/idolchatter/2013/01/24/american-idol-baton-rouge-live-blog/1863097/ (liveblogging a recent episode of *American Idol*); *doctor who liveblog – Tumblr*, Tumblr, http://www.tumblr.com/tagged/doctor+who+liveblog (last visited Jan. 30, 2013) (archiving user-submitted posts with tag "doctor who liveblog," which generally contain responses, quotes, or other content direct from fans actively watching episodes of BBC's *Doctor Who*).

3. Stuart Miles, *Sherlock Sets New Record for BBC iPlayer*, Pocket-lint (Jan. 8, 2012, 11:44 AM), http://www.pocket-lint.com/news/43756/bbc-iplayer-record-new-year-figures.

that a user in the U.S. is located in the U.K. The issue is whether doing so violates copyright law.

The Internet has allowed the world to become increasingly more connected. Though physical borders—and sometimes difficult to surmount digital borders—still exist, the reality is that most things can be obtained online. One side effect of this increased connection is the fact that it is now possible to access copyrighted content that has been placed on the Internet from anywhere in the world, even if that content would not normally be accessible from the user's location. Some of this content is accessed in definitely legal manners—for example, through sites with licenses to make the content available from the copyright holder or sites where the copyright holder has made the content available with minimal restrictions. Other modes of access constitute clear violations of U.S. copyright law, such as when users upload content they do not own, without permission, and make it available for streaming or download.[4] But not all cases are as clean cut. This Note examines one such case. Website operators may provide legally accessible streaming content to users from one location but prevent access by users in others through the use of geolocation tools. A user can, however, convince the geolocation tool employed by the website operator that they are accessing from an authorized location when in fact they are connecting from an unauthorized one.

This Note focuses on U.S. copyright law in answering the question of the potential copyright liability for evading geolocation and in providing a potential solution to the problem of geolocation evasion. Part I discusses how websites can determine the location of their users and how those users can convince the website that they are in fact in an authorized location, with particular focus on Internet protocol ("IP") geolocation. Part II examines the Digital Millennium Copyright Act ("DMCA") and, specifically, the anticircumvention rules in § 1201, considering the approaches taken by circuit courts in anticircumvention cases. Part III suggests a permissive approach to evasion in this context and advocates for licensing agreements as a possible answer to the riddle of evasion of geolocation online for the purpose of accessing a geographically limited, but otherwise legal, stream.

4. For the purposes of this Note, the question of who is properly liable in such cases of clear violations will not be addressed. *See, e.g.*, Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (holding that there was insufficient proof of control to find vicarious liability on the part of Google for copyright secondary infringement); CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 551 (4th Cir. 2004) (analogizing the role of an internet service provider to that of a telephone common carrier as a mere transmitter of information); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (holding that the online bulletin board service operator did not commit direct infringement when users uploaded infringing copies).

I. Internet Territoriality, Geolocation, and Evasion

A. *Bordered or Borderless: Territoriality on the Internet*

The early days of the development of the Internet came with a belief that "cyberspace might challenge the authority of nation-states and move to a new, post-territorial system."[5] But the Internet is no longer a truly borderless means of communication. Instead, it has developed borders similar to those found in the physical world.[6] This shift comes in part from the advent of geolocation technologies that make it possible to determine, to a certain level of precision and reliability, the location from which an individual user has accessed the site in question.

A truly borderless cyberspace as envisioned through much of the 1990s embraces a libertarian ideal of a world where the real-space government is incapable of asserting control over life online.[7] As Lawrence Lessig noted, "The claim for cyberspace was not just that government would not regulate cyberspace—it was that government *could not* regulate cyberspace. Cyberspace was, by nature, unavoidably free."[8] Despite vocal advocates for the lack of territoriality, it did not last.

Cyberlaw has shifted to the regulation of technology by governments.[9] The focus of cyberlaw is on the endpoints of the network where users access digital content.[10] As a result, the Internet is no longer a borderless libertarian paradise. Instead, the laws that regulate the online world have become borderless in that they may be applied to people accessing the Internet regardless of their physical location.[11] Much of the impetus for this change can likely be laid at the feet of businesses unwilling to discard old geographically based business models.[12] In order to perpetuate these business models, companies quickly developed methods of online geolocation in order to determine *where* individuals were accessing their content from, even if they could not determine *who* was accessing it.[13] These business interests often

5. Jack Goldsmith & Tim Wu, Who Controls the Internet?: Illusion of a Borderless World 14 (2006).

6. Dan Jerker B. Svantesson, *"Imagine There's No Countries": Geo-Identification, the Law, and the Not-So-Borderless Internet*, 10 J. Internet L. 17, 20 (2007).

7. Lawrence Lessig, Code Version 2.0, at 3 (2006) ("Even at Yale—not known for libertarian passions—the students seemed drunk on what James Boyle would later call the 'libertarian gotcha': no government could survive without the Internet's riches, yet no government could control the life that went on there.").

8. *Id.*

9. Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. Rev. 323, 348 (2003) ("If version 1.0 of cyberlaw was characterized by the power of technology to regulate, a defining feature of cyberlaw 2.0 is the government regulation of technology.").

10. *Id.*

11. *Id.* at 332.

12. *Id.*

13. *Id.* ("[S]everal companies are rapidly creating new tools that allow for effective (though imperfect) geographic identification on the Internet.").

align with the interests of governments in regulation online. As Geist posits, since "both business and government share a vested interest in bringing geographic borders to the online environment (albeit for different reasons), it should come as little surprise that technologies facilitating geographic identification have so quickly arrived onto the marketplace."[14] Regardless of the reasons for which these tools were initially developed, they allowed governments to engage in varying levels of online enforcement which, in turn, made the lack of borders on the Internet significantly less appealing.[15] Many of the current borders on the Internet exist either because of website operators acting in response to business interests or government regulation.[16] Other online borders, such as those created at the Internet Service Provider ("ISP") or hardware level, prevent any access to significant online content and are often controversial.[17] This Note will focus upon those methods that rely on determining the user's physical location, rather than those that focus on the ISP or hardware level.

B. *Types of Geolocation Tools*

It is clear that geolocation tools are creating borders within the once borderless Internet. There are a number of ways to achieve this goal of locating the user. Current methods include simply asking a user to report their information, looking at the IP address provided to locate users, and using timing-based techniques.[18] Development in geolocation is driven by a number of factors, though targeted advertising is perhaps the most lucrative.[19] Geolocation, however, is not simply used relatively benignly for targeting advertisements or for web analytics; instead, it is also used to pursue legal action in a number of contexts, including copyright infringement.[20]

---

14. *Id.* at 333.

15. *See* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 581 (2012) ("Once governments began to engage in de facto global enforcement on the Internet, the borderlessness of the network no longer appeared to be an advantage, and the desirability of borders began to be re-evaluated.").

16. *See id.*

17. *See id.* at 583 (discussing filtering methods which rely upon content filtering either at the hardware or ISP level). These methods are generally controversial and, in the later case, are used by the more oppressive regimes in today's world. There are arguments that these methods are also in violation of the First Amendment in the United States and the European Union Charter of Fundamental Rights in the European Union.

18. *See* James A. Muir & Paul C. Van Oorschot, *Internet Geolocation: Evasion and Counterevasion*, ACM COMPUTING SURVEYS, Dec. 2009, at 4:1 (discussing means of geolocation, with primary emphasis on IP geolocation).

19. *Id.* at 2. Advertisers will often want to target their online advertisements to the user's location. For example, a local business may only want their advertisements to be served to users within their immediate area, or national retailers may want to include the local address on their advertisements.

20. *See id.* (discussing reasons why a user may choose to evade geolocation online).

1. The Self-Reporting Method of Geolocation

The first type of geolocation, based purely on self-reporting, is the most basic means of locating a user online.[21] While useful for advertising or providing custom content, this method is not particularly valuable as a tool for enforcement.[22] Users can easily falsify their location simply by choosing another option. Or, if the website stores a cookie on the user's computer to save the originally provided location, future relocation of the computer may not be captured. These tools therefore have limited usefulness in the copyright context. These methods are somewhat more reliable than typical self-reporting but are still unlikely to be useful for enforcement purposes.[23] This Note will thus focus primarily on the second type of geolocation, IP geolocation.

2. IP Geolocation

IP geolocation provides a greater degree of reliability than the self-reporting method. Increasing in popularity, IP geolocation is even used by companies such as Google, who automatically redirect traffic based on client IP.[24] This method is particularly powerful because the IP address can often be traced to reveal either the individual user or at least the exact machine used to access the Internet."[25] IP addresses are numeric strings tied to a computer or other device accessing the Internet; they have been likened to real-world mailing addresses.[26] Because the IP address is tied to the device, it is capable of providing some information as to the access location. Yet many current IP addresses are not permanently assigned to a particular device; they are instead assigned on a dynamic, temporary basis.[27] As a result, the same IP address may point to completely different devices depending on when that address is logged. This issue arises because the number of addresses available under IPv4, the currently prevailing IP, has been exhausted.[28] This means that determining the access point is a somewhat more

21. *See* Trimble, *supra* note 15, at 592.

22. *See id.* at 593.

23. *See id.*

24. Muir & Van Oorschot, *supra* note 18, at 4:2.

25. Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 897 (2011).

26. *Id.* at 899–900 ("An IP address is a string of four numbers, each ranging from 0 to 255, that serves as a unique identifier to facilitate online communications. An IP address is tied to a computer, not its user, and will ordinarily not change when a new user logs in. In this way, an IP address is analogues to a physical mailing address, which is required for the sending and receiving of postal mail.").

27. *See* Trimble, *supra* note 15, at 594.

28. *See id.* at 595. The launch of IPv6 will increase the available number of addresses, alleviating this particular problem. The shift from IPv4 to IPv6 skips IPv5 because IPv5 was used to indicate the second iteration of Internet Stream ("ST") Protocol, which initially was thought to be the replacement of the IP system. Ultimately, however, the ST approach did not

complicated process, though the ISP that assigned the address can determine to which account that address was assigned.[29]

Some of the information provided by IP addresses is intentionally recorded in databases by the entity which has registered the address (typically an ISP or other organization).[30] The information in these databases is often provided as contact details for the registrant.[31] It can be accessed through using various identifiers in publicly accessible databases, all of which provide varying degrees of precision and accuracy.[32] In order to find most of the information provided by the registrant, a website operator can run a "whois" lookup[33] on the IP address itself, the autonomous system ("AS") numbers, or the domain name associated with the address.[34] Just as every device will have an IP address when it connects to the Internet, every IP address is associated with an AS number, which is a unique 16-bit integer used for routing.[35] The information provided from the IP address lookup typically includes contact information provided, at least in part, to help users deal with network problems.[36] Similarly, the location information gathered by looking up the AS number provides the point of contact for the registrant of that number.[37] Finally, domain name lookups use the DNS database to provide information for the registrant of the domain name.[38] Absent some act of evasiveness by the user or registered entity (either through falsifying the provided information or intentionally obscuring the correct IP address), this information is generally reliable. Yet even without an intentional act of evasion, these data points are not perfect. Most notably, all of the information accessed here will usually point to an organization or ISP. This means that the entity identified in the lookup's address may not be the same, or even close to, the location of the target host.[39] For example, a lookup of the IP

take hold and IPv5 was never deployed. Brian Robinson, *What Ever Happened to IPv5?*, FCW (July 31, 2006), http://fcw.com/articles/2006/07/31/what-ever-happened-to-ipv5.aspx.

29. *Id.* ("[O]nly Internet service providers know at any given moment which dynamically assigned IP addresses are assigned to which users.").

30. Muir & Van Oorschot, *supra* note 18, at 4:4.

31. *Id.* at 4:4.

32. *Id.* at 4:4–7.

33. A "whois" lookup accesses a public database that provides information that connects various Internet identifiers with the real-world entity that is registered to that identifier.

34. Muir & Van Oorschot, *supra* note 18, at 4:4–6. Though a "whois" can always be run on the IP address provided or the AS numbers, not all IPs will be associated with a domain name. But since domain names must also be registered, a lookup on the domain name, where available, can provide useful information.

35. *Id.* at 4:4–5.

36. *Id.* at 4:4.

37. *Id.* at 4:5.

38. *Id.* The DNS database stores data pertaining to registered domain names. This information includes the reported address of the registrant.

39. *See id.*

address of a user located in Ottawa may reasonably return an address in Toronto, 450 kilometers from the user's actual location.[40]

Lookup by AS number poses similar problems, as some locations indicated by certain AS numbers may have an astronomically smaller population than that indicated by the batch of IP addresses associated with the AS number.[41] The domain name lookups are similarly unreliable because some large Internet hosts may map only to a single location.[42] The registrant may also have voluntarily provided information in the DNS LOC records.[43] Where provided, this information is likely to be more geographically precise than other means, as it provides "latitude, longitude, altitude, size, horizontal precision and vertical precision" which, particularly with regards to the latitude and longitude, can be used to directly map the host location.[44] The information provided could still be falsified or misleading.[45] The advantage of all these approaches is that coding in a "whois" lookup on any or all of these factors is relatively simple and can quickly provide at least semi-reliable information to the website operator.

Not all of the information that comes with an IP address is necessarily provided by the registrant, however. Other data may be collected less directly, such as in the context of geographically limited domain names. Because the domain name–registrant chooses to use a geographically limited or associated domain name, geographically limited domain names share similarities with the previously discussed registrant-provided information available within a "whois" lookup of the domain name.[46] Many of the current top-level domain names ("TLDs") are country-level domains, meaning that the

40. *Id.* at 4:4 ("[O]ne author's IP address in Ottawa falls in the address block 70.24.0.0/13. ARIN lists the registrant for this block as Rogers Cable Inc. (ROCA), One Mount Pleasant, Toronto, Ontario, M4Y 2Y5, Canada. So this technique would geolocate the author's PC (with very poor precision) to Toronto, 450 km from its true Ottawa location (albeit, still with correct country-level resolution)."). ARIN stands for the American Registry for Internet Numbers, a Regional Internet Registry. It coordinates and manages the region's Internet number resources. ARIN's region includes Canada, many of the Caribbean and North Atlantic islands, and the United States. *ARIN at a Glance*, AM. REGISTRY FOR INTERNET NOS., https://www.arin.net/about_us/overview.html (last viewed Mar. 7, 2013).

41. Muir & Van Oorschot, *supra* note 18, at 4:5 (discussing AS 1239, which indicates Reston, Virginia with a population under 100,000 and 2,883,584 associated IP addresses).

42. *Id.* at 4:6 (noting that all hosts with the aol.com domain name map to Dulles, Virginia).

43. *Id.* (discussing the public DNS database but noting that very few hosts have these records). A DNS LOC record provides quite detailed location information for a given domain name.

44. *Id.* The DNS LOC record provides exact coordinates as provided by the registrant. Though this information can be left out or potentially falsified, where available it is significantly more precise than similar information available in other locations.

45. *Id.* at 4:7.

46. *Id.* at 4:7–8 (discussing geographic codes within domain names).

last two letters of the domain name often indicate the country of origin.[47] But even where the domain name–registrant must retain some connection to the indicated country, the registrant's computers may very well be placed elsewhere.[48] Further, not all country code TLDs actually require association with the indicated country.[49] Finally, some countries are simply too large for this form of identification to prove particularly useful.[50]

Still other information is available when pairing the unreliable user-provided information discussed above with data provided by an application used for Internet access and an associated IP address.[51] User-provided information may be rendered somewhat more reliable if it can be associated with the same IP address over time.[52] Application-provided data is somewhat different. Web browser HTTP headers, for example, often include information that can at least somewhat reasonably be inferred to indicate location.[53] A website operator could also use code to request data such as time of day, which will at the very least provide information as to the user's time zone.[54] Though this information is not always available and can potentially be falsified, when paired with an IP address it can provide at least some data as to the location of a user.

3. Time- and Distance-Based Techniques for Geolocation

Measuring the time it takes to get a reply from the host or examining the path it takes to get to the host provide slightly more technical methods of estimating location.[55] It is possible for the website operator to determine the time it takes to send a message to and receive a reply from the host using the

47. *Id.* at 4:7 (discussing the association between a country code TLD and the country indicated). These TLDs have a variety of rules depending on the managing organization and may or may not require the registrant to have some form of presence in the indicated country. For example, Canada maintains geographic requirements for registrants of .ca domain names while the .md domain names, technically for the Republic of Moldova, are marketed to the healthcare industry.

48. *Id.*

49. *Id.* at 4:7–8 (giving the example of the .md TLD, which indicates the Republic of Moldova but is marketed to, and used by, the healthcare industry worldwide).

50. *Id.* at 4:7. In the copyright context, however, if the country indicated by the TLD were reliable as to the location of the computer (which, as discussed above, is not necessarily the case), geolocation even on such an imprecise scale may be sufficient. If the main concern is whether the website operator is in compliance with the copyright laws of a given country or only providing content in a manner permissible under a licensing agreement, the country is likely to be the most important detail.

51. *Id.* at 4:8.

52. Unfortunately, at least for the proponents of online geolocation, dynamically assigned IP addresses make this less likely.

53. *Id.* at 4:8 (noting that "en-GB" in a "User-Agent" string may lead a server to determine that the user is English, from Great Britain).

54. *Id.*

55. *See id.* at 4:8–10.

common command line tool "ping."[56] This information can be analyzed and used with a relatively high level of precision, at least where the host is configured to respond to such a request.[57] But this method has a major drawback. Repeated requests may be viewed as an attack on the host since they create a heavy load on the server, and beyond a certain level they could prevent other access or cause the server to crash.[58] In addition, the tests that have been conducted mostly involve well-connected hosts, and thus the level of precision may be significantly lessened in other contexts.[59]

The remaining method involves drawing inferences based on looking at what other hosts are "near" the target host.[60] This essentially involves tracing the route taken to reach the target host and examining the IP addresses or domains of the hosts nearest in the chain to the target for location information.[61] While results of such a trace may provide information about a host relatively near the target, this is no guarantee of the actual physical distance between the located host and the target.[62] As with all other IP geolocation methods, each of these has its drawbacks and is far from perfect.

C. *Evasion of Geolocation*

Part I.B discusses a number of problems with the various approaches to IP geolocation, including falsification of information. Beyond those limitations, users may also take steps to intentionally disguise or alter their IP address to avoid detection. Not all reasons for evasion are inherently objectionable. Some users may be particularly interested in privacy, for example.[63] Or perhaps a user who grew up in England may simply prefer to view the British version of the BBC news homepage rather than the American

56. *Id.* at 4:8. The command line is a method of issuing commands to a computer which uses a text interface rather than a graphical one. It often allows for more fine-grained control of the computer than a graphical interface would. The "ping" command line tool sends a request to a server and displays a reply that shows the route the message travelled between the remote server and the requesting computer.

57. *Id.* at 4:8–9 (discussing the accuracy of specific methods for using the time to determine location but noting that, increasingly, hosts are configured to not respond to these requests). These methods involve determining the (estimated) absolute minimum round-trip time for the message to be sent and a response received between the requesting server and the user's machine. If this time can be determined, then actual distance and location can be calculated.

58. *Id.* at 4:9 (noting that it is possible to space out the ping requests to avoid this, but doing so greatly limits the real-time usefulness of the method). The server is unlikely to crash when the requests are sent purely to locate individual users accessing the website in a normal manner. The risk of malicious users attacking sites through repeated requests has led server operators to block these requests. In addition, a poorly coded request could potentially loop and cause a similar problem.

59. *Id.* at 4:9 (noting specifically that dialup or satellite connections may be problematic).

60. *Id.* at 4:10.

61. *Id.*

62. *Id.*

63. *Id.* at 4:2.

one. If, however, the evasion allows access to content protected under copyright that would otherwise be inaccessible, then the act may be objectionable under copyright law. Also interestingly, many so-called evasion techniques closely resemble the generally unobjectionable telecommuting practices of business travelers or employees.[64]

Some effective evasion methods are not generally thought of as forms of evasion. Perhaps the simplest evasion technique is one that should be familiar to any business traveler who worked in the hey-day of dialup Internet: dialing long distance to access an ISP.[65] This method is slow and expensive in today's world of high-speed Internet but will almost always be available.[66] In addition, there are services which allow users to remotely access a computer, often a computer owned by the user, located anywhere in the world. If the user then accesses the Internet using this computer, that computer's IP address attaches to their activities.[67] This form of remote access typically requires the user or the user's family or friends to own a computer located in the desired geographical location.[68] A number of remote desktop applications allow use of a remote machine almost as if that machine were sitting directly in front of the user.[69]

There are also techniques with a bit less in common with traditional Internet access methods. One such method is the use of a proxy.[70] A proxy sits between the client and the server being accessed and will usually run on an entirely different host from either; essentially, it is a remote host that the client accesses from their host and then uses to access other places online as if they were located at the remote host.[71] There are a variety of proxy services, the simplest of which are the easiest for concerned websites to block.[72] These are simple webpages on which a user enters the address of the website they wish to access, receiving the requested site within the browser's frame in response.[73] Because website operators can determine the IP addresses used by this sort of proxy, they can generally prevent access through this method if they desire.[74] Yet these are not the only forms of proxy service. There are also a number of subscription services, either specialized by coun-

64. *See infra* notes 61–75 and accompanying text.
65. Trimble, *supra* note 15, at 601.
66. *See id.*
67. *Id.* at 600–01 (identifying LogeMeIn and GoToMyPC as examples).
68. *See id.* at 601 (describing this method as "self-sustained" cybertravel).
69. *See* Muir & Van Oorschot, *supra* note 18, at 4:14.
70. *See id.* at 4:13–14 (discussing use of proxies).
71. *Id.*
72. *See* Trimble, *supra* note 15, at 602.
73. *Id.*
74. *Id.* These proxies are identifiable because the requests will come from certain IP addresses that are available to the proxy service. As a result, website operators can simply block the IPs known to be used by the service.

try or covering larger regions, which provide proxy access to paying users.[75] These services provide a range of benefits to the user who wants to evade geolocation, from increased privacy to the ability to access blocked content.[76] The Tor project, provided for free to users, is likely the most significant proxy service. It "utilizes a series of proxies," and political activists, whistleblowers, and intelligence gatherers use it heavily.[77] Notably, the U.S. government generously funds this particular project.[78] Similar in a technical sense, using SSH, or Secured Shell, to access a remote machine and then accessing the Internet from that machine also constitutes using a proxy. This method is not as useful as Tor, however, because the user or someone connected to them generally must have control over the machine being used and access is only text based.[79]

Even as geolocation tools become more accurate, users will continue to find ways to evade these measures.[80] There are options for website operators that may be useful in locating users even where the user hides their host IP, but as with the IP geolocation tools, these are imperfect and lack precision.[81] It seems possible that other means may supplant IP geolocation as the primary method of determining the location of users in the future, but it is substantially more likely that new techniques will be developed to evade the use of those tools.[82]

As will be discussed further in Part III.C, geolocation tools are useful to copyright holders and website operators in the licensing context. Ultimately, despite the possibility of evasion, a reasonably reliable geolocation tool serves as a valuable method of "effective regulation and enforcement on the Internet" and can aid business entities looking to divide markets and grant licensing rights in one country while withholding them in another.[83] From the business perspective, not all groups interested in licensing content may be able to pay for a world-wide license.[84] As a result, market segmentation makes licensing opportunities available to a wider range of licensees.[85] In

75. *See id.* at 602–03 (mentioning Anonymizer and My Expat Network as examples).
76. *Id.*
77. *Id.* at 603–04.
78. *Id.* at 603.
79. Muir & Van Oorschot, *supra* note 18, at 14 ("Anyone with ssh access to a remote machine (e.g. anon.machine.example) can, through port forwarding, use this machine as a SOCKS proxy to browse the web through.").
80. *See* Trimble, *supra* note 15, at 604 ("As one might expect, this is a constant race where it may take just a few weeks or months for the creators of evasion techniques to respond to improvements in geolocation tools and improve their techniques to further challenge geolocation.").
81. *See id.*
82. *See id.* at 605 (mentioning GPS location information as a possible substitute).
83. *Id.*
84. *Id.*
85. *Id.*

addition, the copyright holder is able to maximize their profits by choosing the most beneficial licensing arrangements.[86]

II. The Legal Landscape

A. *Copyright Territoriality and Geographic Limitations*

Copyright law, though in many ways harmonized through international treaty, remains a highly territorial regime.[87] It is this territoriality, from both legal and licensing perspectives, which makes geolocation a useful tool for website operators. The license obtained by the website operator to make content available for streaming online may well be restricted to a certain country or countries by the copyright holder.[88] One entity might hold the copyright in all the countries in question for a variety of reasons, including financial constraints, copyright holder preferences, or a desire to control price or release date in different geographic regions.[89] In certain situations, exclusivity agreements with distributors may limit licensing availability. Yet in other scenarios, the copyright holder may differ in various countries and the rights-holders in some countries may be unreachable or unwilling to agree to a streaming license.[90]

Though different in a number of ways, the online streaming context shares some similarities with the controversy over region-coded DVDs.[91] Both region encoding and geographically restricted streaming use the (presumed) location of the viewer to limit access to the copyrighted work and raise concerns under § 1201 of the DMCA, which provides the anticircumvention rules.[92] The two contexts are perhaps the most similar when a user has paid for access to a stream but cannot view it because of their location. Even the grounds typically cited for the two sets of restrictions reflect a high degree of similarity: DVD region encoding is generally attributed to staggered release dates, price discrimination, distribution and licensing agreements, and regulatory standards or censorship issues.[93] Professor Peter Yu

86. *Id.*

87. *See* Peter K. Yu, *Region Codes and the Territorial Mess*, 30 Cardozo Arts & Ent. L.J. 187, 188 (2012).

88. *See* Trimble, *supra* note 15, at 611.

89. *Id.*

90. *Id.*

91. DVDs often include a form of digital rights management which divides the world in to six regions. A DVD with region 1 (consisting of the U.S. and Canada), for example, is playable only on DVD players capable of reading the region 1 encoding. This means that someone in the U.K. is unlikely to be able to play such a DVD. Because the region encoding system divides the playability of the content geographically, it is similar to the geographic limits imposed by geolocation tools.

92. 17 U.S.C. § 1201 (2011).

93. *See* Yu, *supra* note 87, at 199–216 (describing the justifications for or benefits of region encoding).

states that only staggered release actually justifies encoding,[94] a theory which may not apply as cleanly to online streaming. While censorship and price discrimination may raise concerns in both contexts,[95] licensing agreements are likely to be of much greater concern where no physical copy is sold to the viewer. This is partially due to the fact that the sale of a physical copy clearly triggers the first-sale doctrine with regards to the copy sold while the lack of sale of a copy inherent in the digital streaming context does not.[96] As a result, the argument for limiting access to a stream geographically is somewhat stronger than the arguments advanced for region encoding of DVDs. Internet geolocation tools, at least to the extent that they are reliable, are also less arbitrary than the current DVD regions. It is possible to allow or block single countries (or potentially even narrower geographic units) from access using many of the available tools. In this manner, for example, Hong Kong may be treated as part of China by a geolocation tool, whereas DVD regions would mean a disc playable in a Hong Kong DVD player was not playable in China and vice versa.[97]

B. *DMCA § 1201: The Ban on Circumvention of Access Controls and Trafficking in Circumvention Tools*

Copyright holders have specific rights in their works. These rights include the right of reproduction, the right to prepare derivative works, and the right to distribute copies or phonorecords of the work.[98] In addition, the holders of copyrights in certain categories of works have the right of public performance (in the case of sound recordings, the right of public performance by digital audio transmission) and the right of public display.[99] Along with these rights, § 1201 prevents circumvention of access or copy controls placed on the copyrighted work.[100] Passed as part of the DMCA in 1998, the anticircumvention rules in particular were intended to bring U.S. law in line with treaty obligations under the World Intellectual Property Organization

94. *Id.* at 216 ("Out of the four justifications advanced in this Part, only sequential release provides a convincing justification for DVD region codes. It is therefore no surprise that DVD CCA includes only the first justification in its explanation of the need for region codes.").

95. Specifically, censorship is likely to raise First Amendment concerns in the U.S. and price discrimination is of concern under antitrust laws.

96. 17 U.S.C. § 106(3) (2011); 17 U.S.C. § 109(a) (2011) ("Notwithstanding the provisions of section 106 (3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.").

97. *See, e.g.*, Yu, *supra* note 87, at 234 (noting that Hong Kong, now a part of China, is region 3 while China is region 6).

98. 17 U.S.C. § 106 (2011).

99. *Id.*

100. *Id.* § 1201.

("WIPO") Treaty.[101] Section 1201(a) of the DMCA bans the act of circumventing any measure that "effectively controls access to a work protected under [the] title" as well as the trafficking in devices for this purpose.[102] It is these provisions that could be violated whenever a user evading Internet geolocation in any of its forms accesses otherwise inaccessible copyrighted content on the Internet. In addition, liability potentially exists for the parties who created the tools[103] used by these end users under the trafficking portion of the provisions. This Note focuses primarily on whether a user in the U.S. runs afoul of the restrictions in § 1201 when using a proxy or other geolocation evasion method to access an otherwise lawful but geographically restricted stream. If the answer is affirmative, it is also necessary to determine whether there are any limitations on the applicability of § 1201 in this context, and additionally, whether the developers and providers of evasion tools may be held liable as traffickers of circumvention devices under § 1201(a)(2).

1. Exceptions to § 1201(a) Liability

It is important to note that even if courts read § 1201 strictly, exemptions do exist that allow certain acts of circumvention.[104] None of the specific exceptions provided cover the evasion of geolocation online unless the data collected to establish the location of the user can be defined as personally identifying information ("PII").[105] Subsection (i) provides in part that:

> (1) Circumvention permitted. 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[.]

Thus, if the geolocation data—particularly when paired with other data collected by the website operator about the user—can be viewed as PII, then

101. *See* Lev Ginsburg, *Anti-Circumvention Rules and Fair Use*, 2002 UCLA J.L. & TECH. 4.

102. 17 U.S.C. § 1201(a) (2011); *see also* Eddan Elizafon Katz, *Anticircumvention Provisions:* RealNetworks, Inc. v. Streambox, Inc. & Universal City Studios, Inc. v. Reimerdes, 16 BERKELEY TECH. L.J. 53, 53 (2001); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 471–72 (2003).

103. For example, if 17 U.S.C. § 1201(a)(2) creates liability for manufacturers and providers of geolocation evasion tools, the Tor Project would be illegal under the Copyright Act.

104. 17 U.S.C. § 1201 (2011) (establishing specific exceptions for certain situations or groups, such as reverse engineering or law enforcement, and also establishing the power of the Librarian of Congress to make exceptions to § 1201(a)).

105. *Id.* § 1201(i).

the act of circumventing geolocation is not in violation of § 1201(a). For example, if the website operator is able to pair the IP address with consistent site activity or information provided by the user in the creation of an account, it is quite possible that the website operator can individually identify that user in their visits. If this is the case, then the user's desire to prevent this identification would likely fall under § 1201(i).

In addition to the statutorily defined exemptions, it is possible for the Librarian of Congress to create an exception that lasts for three years for a particular type of circumvention.[106] The most recent Librarian of Congress–made exceptions were codified in the Federal Register on October 26, 2012.[107] Yet none of these currently established exceptions apply to the evasion of geolocation; most exceptions, though not all, relate to accessibility in the case of disability or to interoperability.[108] These exceptions, described as a "fail-safe," are intended to offset negative effects in the marketplace from the requirements of § 1201.[109] During the proceeding to establish the three-year exceptions, the Register of Copyrights and the Librarian of Congress are supposed "to assess whether the implementation of access control measures is diminishing the ability of individuals to use copyrighted works in ways that are not infringing and to designate any classes of works with respect to which users have been adversely affected in their ability to make such noninfringing uses."[110] Even when a class of works has been granted an exception under a previous rulemaking, there is no assumption that such an exception should be renewed.[111] It is up to the group proposing an exception to convince the Register and Librarian that the exception is warranted.[112] In addition, there must be a showing of harm by the law to the alleged noninfringing use in order for an exception to be granted.[113] In the latest rulemaking, five exceptions were granted and four other exceptions were considered but denied.[114] The currently excepted classes include: literary works distributed electronically for the purpose of assistive technologies; wireless telephone headsets for the purpose of software interoperability;

106. *Id.* § 1201(a)(C).

107. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access and Control Technologies, 77 Fed. Reg. 65260 (Oct. 26, 2012) (codified at 37 C.F.R. part 201), *available at* http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

108. *Id.*

109. U.S. Copyright Office, Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights, at 4 (Oct. 2012), *available at* http://www.copyright.gov/1201/2012/Section_%201201_%20Rulemaking%20_2012_%20Recommendation.pdf.

110. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access and Control Technologies, 77 Fed. Reg. 65261 (Oct. 26, 2012) (codified at 37 C.F.R. part 201), *available at* http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.* at 65262–77.

wireless telephone headsets for the purpose of interoperability with alternative networks; motion picture excerpts for the purpose of commentary, criticism, and educational uses; and motion pictures and other audiovisual works for the purpose of captioning and descriptive audio.[115] One of those exceptions, the one in place for wireless telephone headsets for interoperability with alternative networks, is an extremely limited exception which only applies to "handset[s] originally acquired from the operator of a wireless telecommunications network or retailer no later than ninety days after the effective date of this exemption."[116] None of these current exceptions resemble the issue of evasion of geolocation. It seems unlikely that such an exception would be forthcoming from the next rulemaking (presumably in 2015) in this context. Although it is possible that privacy or free speech advocates might lobby for the freedom to circumvent geolocation, such an exception appears to sweep more broadly than the Librarian has previously allowed.

If no Librarian of Congress exceptions are forthcoming and the PII exception in subsection (i) does not apply, then it remains possible that users of geolocation tools who access geographically restricted streams are acting in violation of § 1201(a). As discussed in Part III.B, this is particularly troubling for users who may not realize that such behavior is prohibited in the statute or who are using the evasion tools primarily for a purpose other than accessing these streams, such as for greater privacy or to access a remote machine. If a user often accesses the Internet via proxy, for example, they may not even realize that by using their ordinary IP address they would be unable to view specific streaming content.[117]

2. Trafficking in Circumvention Devices

Section 1201(a)(2) of the DMCA provides that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" which allows the user to circumvent an access control.[118] This subsection explains that where the device trafficked in and used for circumvention "(A) is primarily designed or produced for the purpose of circumventing . . . or (B) has only limited commercially significant purpose or use other than to circumvent . . . or (C) is marketed . . . for use in circumventing a technological measure that

115. *Id.* at 65262–71.

116. *Id.* at 65264.

117. In a conversation with friends living in Canada, for example, I discovered that until very recently *Star Trek: The Next Generation* ("*Star Trek*") was not available on Netflix in Canada. If I were visiting Canada and, using remote access tools, logged onto Netflix through a U.S. computer and watched an episode of the show, that could amount to an entirely unknowing and unintended violation of § 1201(a). This could be the case even if I were using the remote access for reasons entirely unrelated to viewing *Star Trek* in Canada and was entirely unaware that I could not have watched *Star Trek* from a computer located in Canada.

118. 17 U.S.C. § 1201(a)(2) (2011).

effectively controls access to a work protected under this title," then the sale or other provision of that device is prohibited.[119]

As discussed above, however, geolocation evasion tools have many uses. It is unlikely, for example, that military groups or law enforcement make use of the Tor Project simply to access copyrighted materials that they could not otherwise access.[120] The same can be said for most other evasion technologies. Remote access and long distance dialup have been in use for longer than geographically limited video streams have been available online. As a result, it seems likely that—short of a particular marketing scenario—the developers or providers of such devices should remain free from liability.

3. The Ninth Circuit Approach

In *MDY Indus. v. Blizzard Entertainment, Inc.*, the Ninth Circuit found it significant that § 1201(a) does not "explicitly refer[ ] to traditional copyright infringement under § 106" while the text of § 1201(b) does.[121] The Ninth Circuit there held that "while §1201(b) of the Copyright Act is bound to an act of copyright infringement, §1201(a) creates liability for circumvention per se."[122] Under this interpretation, any act of circumvention of an access control—even one that results in no infringement on any of the rights of the copyright holder—is in violation of § 1201(a). Further, this interpretation does not subject this new right to limiting doctrines such as fair use.[123]

As a result, the court read the statute "as extending a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to works protected under Title 17, i.e., copyrighted works."[124] *MDY Indus.* dealt with a situation where there did not appear to be any violation of the traditional rights of the copyright holder; specifically, it involved a bot developed for cheating on World of Warcraft ("WoW") that avoided detection by the game's systems.[125] In fact, in discussing the bot (called Gilder), the

---

119. *Id.*

120. *Users of Tor*, Tor Project, https://www.torproject.org/about/torusers.html.en (last visited Dec. 30, 2012).

121. MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 945 (9th Cir. 2010).

122. Trimble, *supra* note 15, at 618; *see also MDY Indus.*, 629 F.3d at 928; Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 294 (S.D.N.Y. 2000).

123. Trimble, *supra* note 15, at 618–19 ("The Ninth Circuit's interpretation therefore recognizes section 1201(a) as creating a new 'right to permit access to copyrighted work,' a right that is not among the exclusive rights that copyright holders traditionally enjoy and that is not—as opposed to the exclusive rights enumerated in section 106 of the Copyright Act—subject to the fair use doctrine."). 17 U.S.C. § 107 provides for fair use exceptions to the rights of the copyright holder found in 17 U.S.C. § 106. If a use is found to be a fair use, it is considered to be non-infringing. The statute directs courts to consider "the purpose and character of the use . . . the nature of the copyrighted work . . . the amount and substantiality of the portion used and . . . the effect of the use on the potential market."

124. *MDY Indus.*, 629 F.3d at 945.

125. *Id.* at 935–36.

court noted that "Gilder does not alter or copy WoW's game client software, does not allow a player to avoid paying monthly subscription dues to Blizzard, and has no commercial use independent of WoW."[126] Even if the court's findings as to the meaning of § 1201(a) were unclear—which they are not—the outcome of the case essentially means that no relationship between a violation of a traditional copyright right and the act of circumvention is necessary to find a violation of the subsection.

Decided prior to *MDY Indus.*, *Universal Studios v. Reimerdes* is an anticircumvention case from the Southern District of New York. The *Reimerdes* court adopted the same approach that would later be followed by the Ninth Circuit.[127] The case concerned the distribution of DeCSS, a program which allowed users to circumvent access restrictions on a DVD and to play that DVD on a non-licensed player.[128] In substance, the conclusion in *Reimerdes* is the same as that in *MDY Indus.*[129] Yet *Reimerdes* provides additional insight into an important question when considering evasion of geolocation. Specifically, the court deals with the question of how "effective" the access control must actually be.[130] The court, in analyzing the legislative history, finds that "a technological measure 'effectively controls access' to a copyrighted work if its *function* is to control access."[131] This is significant because, as discussed in Part I, no geolocation tool is perfect. Under the approach in this case, however, a geolocation tool clearly "effectively" prevents access.

It is evident then that, under the approach espoused by the Ninth Circuit and by at least one District Court in the Second Circuit, evasion of geolocation in order to access otherwise lawful streaming content is a violation of § 1201(a).[132] As a result, unless an exception applies, such evasion would be considered unlawful under any circumstances, should this interpretation prevail. It is worth noting that both of these cases deal with the trafficking provisions of § 1201(a)(2) and not the actual anticircumvention provisions.[133] But, for the purposes of determining whether traditional infringement is necessary, the question remains the same in both cases. In each instance, § 1201(a) is a matter of strict liability.

126. *Id.* at 935.
127. *Reimerdes*, 111 F. Supp. 2d at 294.
128. *Id.*
129. *See id.*
130. *Id.* at 317–18.
131. *Id.* at 318.
132. *See* Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 945 (9th Cir. 2010); *Reimerdes*, 111 F. Supp. 2d at 294.
133. *Id.*

4. The Federal Circuit Approach

Another core case on the anticircumvention rules—*Chamberlain Group, Inc. v. Skylink Tech, Inc.*, from the Federal Circuit—concerns the manufacture of garage door openers.[134] Chamberlain manufactured garage door openers that used copyrighted "rolling code" which constantly changed the signal needed to open the door.[135] Skylink manufactured substitute remote controls for the garage doors that did not incorporate this rolling code.[136] As in the previous cases, *Chamberlain Group, Inc.* deals with trafficking liability under § 1201(a)(2).[137] Yet the Federal Circuit disagrees with the Ninth Circuit on the question of per se liability for circumvention.[138] They note that "[w]ere § 1201(a) to allow copyright owners to block all access to their copyrighted works, it would effectively create two distinct copyright regimes."[139] This would be a drastic change from the prior law.[140] In addition, they note that "[s]uch a regime would be hard to reconcile with the DMCA's statutory prescription that nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title. A provision that prohibited access without regard to the rest of the Copyright Act would clearly affect rights and limitations, if not remedies and defenses."[141] Ultimately, the Federal Circuit finds that "§ 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[142] As a result, the conclusion of the Federal Circuit is quite different from that of the Ninth Circuit. While the Ninth Circuit approach renders any act of circumvention of access controls a violation of § 1201, the Federal Circuit requires at least some nexus between that circumvention and the underlying copyrighted work.

5. The WIPO Treaty and European Law

Article 11 of the WIPO Copyright Treaty requires that "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which

134. The Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).
135. *Id.* at 1183.
136. *Id.*
137. *Id.* at 1178.
138. *Id.*
139. *Id.* at 1199.
140. *Id.*
141. *Id.* at 1200 (internal quotation marks omitted).
142. *Id.* at 1202.

are not authorized by the authors concerned or permitted by law."[143] Under the language of the treaty, then, the concern is not purely whether access controls are circumvented, but whether the anticircumvention tool (here geolocation) is used to prevent acts "which are not authorized by the authors concerned or permitted by law."[144] Of course, this raises the question of what the reach of "authorized by the author" is in the geolocation context.[145] But Article 11 does not facially require that all contracting parties make any act of circumvention of access controls a violation of the copyright laws. The anticircumvention measures of the DMCA, as well as those measures implemented in European law, were intended to give effect to these treaty obligations.[146]

The Federal Circuit approach to the DMCA, discussed in Part II.B.4, is similar to the approach taken in Europe in implementing the WIPO Treaties.[147] As implemented in the 2001 EU Information Society Directive, European law "require[s] that circumvention of technological measures be associated with a committed or potential unauthorized or illegal act."[148] Specifically, the Directive provides that member states should "allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases."[149] Under the U.K. implementation of the Directive, there is no liability for an act of circumvention of access controls unless that act of circumvention facilitates an act of copyright infringement.[150] It is possible to classify the act of accessing a stream from a location outside of the authorized geographic region as "unauthorized," but the stream itself is authorized by the copyright holder, as is the act of viewing it. European law provides for a more flexible approach to anticircumvention than that taken by the Ninth Circuit (or S.D.N.Y.) in the U.S. and potentially even that which is available under the Federal Circuit approach. Even though European law does not aid in interpreting U.S. law, it is a helpful indicator of what other parts of the world view as reasonable with regard to the question of circumvention.

143. World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 [hereinafter WIPO Copyright Treaty].

144. *Id.*; *see* Trimble, *supra* note 15, at 612–13.

145. WIPO Copyright Treaty, *supra* note 143.

146. *See* Trimble, *supra* note 15, at 612–15.

147. *See id.* at 613–14 (discussing European implementation of the WIPO treaties and the EU Information Society Directive).

148. *Id.* at 614.

149. Council Directive 2001/29, art. 47, 2001 O.J. (L 167) 10, 19 (EC).

150. *See* Trimble, *supra* note 15, at 614–15.

III. Recommendations for Liability in the Geolocation Context

A user who simply views otherwise legally available streaming video is not downloading a permanent copy of the video.[151] It would be somewhat absurd for the copyright holder to argue that any temporary copy created in order for the stream to play on the end user's computer is a violation of their copyright since the same copy would be created by any viewer, even one who is not evading geolocation. Barring a situation where the user plays the stream in public and thus violates the copyright holder's public performance right, the user is not engaging in any of the practices that we traditionally think of as copyright violations.[152] What they are doing is lying about their location. Although this may facilitate access to otherwise inaccessible materials, it is not a question that copyright law should address.

Despite the existence of both rational business reasons for market segmentation and scenarios in which licenses may require that a licensee must at least attempt to limit from which locations a stream is accessed, there should not be copyright liability for a user simply viewing the stream from outside of the desired geographic area. A combination of privacy concerns (discussed further in Part III.A) and concerns over potentially innocent infringement (discussed in Part III.B) make limiting the potential for liability a better approach. Most importantly, geolocation data can and should be considered PII under § 1201(i), allowing users to circumvent the collection of said data. Further, even if this data is somehow collected in a manner that does not render it PII, the European approach (and similar Federal Circuit approach) is far preferable to that taken by the Ninth Circuit.

A. *Geolocation Data Should Be Considered PII*

As of now, federal law does not address the use of geolocation.[153] However, the Federal Trade Commission ("FTC") 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."[154] Level of precision is therefore important. A geolocation tool that could only locate within a city block, for example, would not result in data detailed enough to be considered PII. Some geolocation

151. It is certainly technologically feasible for someone to access streaming content and simultaneously download a permanent copy to their computer, but that is outside the scope of this Note. Such actions would almost certainly result in a copyright violation without turning to § 1201.

152. 17 U.S.C. § 106(4) (2011).

153. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 Alb. L.J. Sci. & Tech. 61, 115 (2011).

154. Fed. Trade. Comm'n, Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology 1, 20 n.47 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

tools therefore do not result in the collection of PII. Where geolocation tools do collect PII, however, evasion of geolocation is clearly not in violation of § 1201(a) as discussed in Part II.B.1. The fact that some geolocation tools do not collect data precise enough to be considered PII does not mean that they all lack this precision. More importantly, most sites collect a variety of information about visitors, not simply their location. Once aggregated, this data may well be sufficient to identify an individual. In the area of behavioral advertising, consumer and privacy groups have pushed to extend the application of FTC principles—usually applied only to PII—to information such as IP addresses.[155] The FTC noted that there are a variety of situations in which IP addresses coupled with other data may be able to identify a specific person, and thus—at least for the purpose of self-regulatory principles—IP addresses should be considered similarly to traditional PII.[156]

If the FTC treats IP addresses similarly in some instances to PII, does that mean those addresses should fall under the legal definition of PII? At least in some cases, the data is sufficient to identify a single user.[157] In fact, if a user's device has a GPS chip, the location data can be extremely precise.[158] Although few websites currently access GPS data, as GPS-enabled phones and tablets become more popular, this method seems likely to become more commonplace than the IP geolocation discussed in Part I.C. This form of geolocation almost certainly collects PII. IP geolocation is a step removed, certainly, but can still be extremely precise and the greater the level of precision, the more likely it is for the information to constitute PII. It has been argued that IP addresses constitute personal data under European Community ("EC") law.[159] Much like the concept embodied in PII, EC law is concerned with the probability of identification.[160] As the accuracy of the geolocation method used goes up, so too does the likelihood that EC law would view its collection and use with concern.[161] Similarly, IP addresses may fall under the definition of "personal information" in the Children's Online Privacy Protection Act of 1998 ("COPPA").[162] Both telephone numbers and email addresses are listed as "personal information" under COPPA

155. *Id.* at 21 ("[A] number of consumer and privacy groups expressed support for applying the Principles to data typically considered to be non-PII. Specifically, these commenters would apply the Principles to such data as Internet Protocol (IP) addresses, cookie data, and other information that the commenters stated could allow a set of behaviors or actions to be associated with a particular individual or computer user, even if that individual is never identified by name.").

156. *Id.* at 21–26.

157. *See* King, *supra* note 153, at 119–22.

158. *Id.* at 121.

159. Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. Marshall J. Computer & Info. L. 101, 135 (2004).

160. *Id.* at 135–36.

161. *Id.*

162. *Id.* at 136; *see* 15 U.S.C. § 6501.

and the Act also provides for determination of other such identifiers. Similarly to IP addresses, email addresses and phone numbers are likely to be used by multiple individuals, so it is reasonable to believe that IP addresses may be included.[163]

Websites that use geolocation tools may well collect more than just the user's location. Further, location alone is a significant piece of identifying information. Finally, and perhaps most importantly, users will not know the level of precision in any given site's geolocation technology or what other information that site has to connect to the location data and use to identify them. It has been suggested that in the criminal context, the sort of geolocation data provided by GPS—which is not drastically different from that provided through the more accurate means of IP geolocation, such as DNS LOC—may in fact represent a cognizable constitutional ill.[164] Though private use of such data would not present the same constitutional concern, it is worrying because the constitutional concern centers around the identifying nature of the data. As a result, geolocation data should be considered PII and thus geolocation technologies should be subject to the exception found in § 1201(i). With circumvention of these tools now allowed under the exception, users can utilize geolocation evasion tools to access streaming content despite geographic restrictions imposed by the website operators unless the website operators meet the notification requirements in the exception. Because website operators can avoid falling within the exception through providing proper notification, allowing it to apply causes at most minimal inconvenience to the website operators.

B. *Even in Cases Where the § 1201(i) Exception Does Not Apply, U.S. Courts Should Adopt an Approach Similar to the European or Federal Circuit Approach*

European law and the reading of § 1201(a) by the Federal Circuit both generally require some form of connection between the circumvention of access and the violation of a traditional copyright right. The European approach to anticircumvention is more flexible than the Ninth Circuit approach, and potentially more so than the Federal Circuit approach.[165] While

163. 15 U.S.C. § 6501.

164. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 167–68 (2012) ("Echoing the conclusions hinted at by the history of surveillance, its coercive utility, and the rapid innovation in contemporary surveillance technology, including geolocation systems, Seventh Circuit Judge Flaum, while criticizing the reasoning of Maynard in Cuevas-Perez, suggests that the fact of the 'government's gaze' itself, as exerted by 'mass use of GPS technology,' may represent a 'constitutional ill' which amounts to a cognizable harm.").

165. Markus Fallenbock, *On the Technical Protection of Copyright: The Digital Millenium Copyright Act, the European Community Copyright Directive and Their Anti-Circumvention Provisions*, INT'L J. COMM. L. & POL'Y, Winter 2002/2003, at 4, 38.

facially § 1201 reads as having no knowledge requirement, the European approach does have a knowledge requirement for the liable party.[166] Though not entirely settled, it is also significantly easier to read in the requirement of a connection between infringement and circumvention in the European approach.[167]

The more flexible European approach is more reasonable. Some flexibility is needed when applying a complex legal scheme to users who may only have the most rudimentary understanding of that scheme. The anticircumvention rules are far removed from what the common citizen would think of as covered under the copyright laws and therefore have the ability to create ridiculous results when applied too strictly. Access for "unauthorized" uses would still be restricted under the WIPO treaty.[168] But if a use is not otherwise illegal, then the user should be made aware that their access is not allowed because of the wishes of the copyright holder. This would protect innocent infringers.

The Federal Circuit noted that having no connection between "action" and "protection" in the context of § 1201(a) "would lead to a result so bizarre that Congress could not have intended it."[169] Though they were talking about garage door openers and computer code, the same logic applies in online streaming. The copyright holder or licensee has made the content available, whether for free or for fee, and a consumer wishes to view it. A savvy consumer knows that peer-to-peer or other download options are probably illegal. Those who want to pay or at least have their view counted by the content creator may decide to access the content in what seems like a reasonable and legal manner. Here, that manner consists of watching the stream that has been made available to at least some part of world and paying the fee, if any, that the copyright holder or licensee collects. The viewer in this case is hardly a pirate depriving the copyright holder of the reward for their creativity. At worst, they are lying and preventing the copyright holder from engaging in market segmentation.

C. *What Can Copyright Holders and Licensees Do?*

In many cases, copyright holders and licensees should not be overly concerned. Not all users will be able or motivated to evade geolocation to access region-locked material online. Some viewers will successfully access the stream from an unauthorized location, but if the stream requires pay-for-view then the website operator will still collect payment for the consumer's enjoyment of the content. If the stream is free, there may be more cause for

166. *Id.* at 39.

167. *Id.* at 40–42 (discussing Article 6 of the Directive and the readings by the Council and Commission).

168. WIPO Copyright Treaty, *supra* note 143.

169. The Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004).

concern, though the consumer is still increasing the number of views and watching any advertising content displayed with the stream. Nevertheless, there are some approaches for those who are particularly concerned with these situations.

First, § 1201(i) only operates where the website operator has not notified the visitor of the data's collection.[170] Use of such a notice is beneficial to the website operator who wants to restrict access, but also to the website visitor who may not realize that their access is problematic. Most online user agreements can either be considered "clickwrap" or "browsewrap" because they come in standard form without negotiation, much like a traditional shrinkwrap agreement.[171] Clickwrap agreements require users to actually click to show their acceptance of terms, while browsewrap agreements make further browsing the act of acceptance.[172] Clickwrap agreements have been held more consistently enforceable than browsewrap because the act of assent by the user is arguably clearer.[173] Potentially, the notice could be as simple as a pop-up window notifying the user that the site is collecting location data to meet copyright licensing requirements and asking the user to acknowledge that their location is, to the best of their knowledge, accurately presented. It could also be included in a standard End User License Agreement in the case of sites such as Netflix, where some form of contractual privity already exists. If the terms are reasonably provided to the user, then there is some duty in the user to read them and abide by them.[174] At least in this context, the consumer who is not evading geolocation purely for access to the specific stream now has some constructive knowledge that their point of access is being collected and thus may be relevant. Ideally, this notification or agreement would also describe the reason for which the information is being collected, notifying users that if they disguise their location from the website, their access is unauthorized, putting it more clearly within the reach of the WIPO treaty. Without this information, the user may potentially be innocently achieving this unauthorized access, unaware that what they are doing is wrong. Subsection (i) also only applies to the act of circumvention, not the trafficking provisions.[175] This is less relevant in this particular context, however, since current geolocation evasion tools have uses other than circumventing access restrictions to copyrighted works.

---

170. *See id.* at 29.

171. Woodrow Hartzog, *Website Design as Contract*, 60 Am. U. L. Rev. 1635, 1642 (2011).

172. *Id.*

173. Ty Tasker & Daryn Pakcyk, C*yber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 Alb. L.J. Sci. & Tech. 79, 96–97 (2008) (discussing the enforceability of contract types and noting that some website operators may still choose browsewrap despite the enforceability risks because of concerns over decrease in traffic when using clickwrap).

174. Hartzog, *supra* note 171, at 1643–44.

175. *Id.*

Second, user agreements can serve a similar purpose as notification to indicate the collection of location data, at least from the perspective of the website operator. If a user must agree that they are accessing the stream from within the defined geographic area, then viewers who are not liable under § 1201(a) are still in breach of the contract created by the user agreement.

Conclusion

Technologically, there is no way to completely prevent evasion of geolocation, and the copyright laws are not the proper place for the handling of such issues. Evasion of geolocation serves a range of purposes and as a result, legal limitations should be carefully considered before being put in place. One of the key purposes served is protection of privacy, which is also one of the key reasons that evasion of geolocation should not be considered a violation of § 1201(a). As discussed in Part III.A, as the accuracy of geolocation tools improve, protection of IP addresses helps to prevent precise identification of users, preserving some level of anonymity. Though anonymity is not always necessary, there remain situations in which higher levels of privacy serve a valid end. For example, journalists may wish to keep their identity secret when speaking with whistleblowers online, while governments may want to preserve privacy in information gathering.[176] In 2009, the Electronic Frontier Foundation encouraged readers to set up Tor bridges or Tor relays to aid Internet users in Iran in circumventing government censorship and to preserve anonymity during the events following the disputed Iranian election.[177] Still other users may wish to avoid "Internet filtering" established by their governments to prevent supposedly harmful information from reaching their citizens.[178] The paradigmatic example of this is perhaps the "Great Firewall of China," but Australia, the EU, and the U.S. have at times proposed legislation that would work similar, though less restrictive limitations on access.[179] If evasion of geolocation wherever copy-

176. *Tor Overview*, Tor Project, https://www.torproject.org/about/overview.html.en (last visited Mar. 19, 2013).

177. *Help Protestors in Iran: Run a Tor Bridge or a Tor Relay*, Electronic Frontier Foundation (June 29, 2009), https://www.eff.org/deeplinks/2009/06/help-protesters-iran-run-tor-relays-bridges.

178. Joanna Kulesza, *Walled Gardens of Privacy or "Binding Corporate Rules?": A Critical Look at International Protection of Online Privacy*, 34 U. Ark. Little Rock L. Rev. 747, 761–62 (2012).

179. *Id.* at 762 ("Apparently encouraged by China's success in delimiting the 'Chinese cyberspace' with the Great Firewall of China, the EU considered the electronic Schengen zone in 2011, the very same year Australia introduced plans to block illegal content away from its 'virtual territory.' Just recently the U.S. considered closing 'U.S. cyberspace' to prevent copyright violations with the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA). The U.S. is still considering securing 'the U.S. cyberspace,' as if raising national borders in cyberspace was a natural consequence of state sovereignty.").

righted content is blocked by geolocation tools is a violation of § 1201(a), then even users who practice evasion for these potentially laudible goals will find themselves running afoul of the statute.

There are valid reasons for a copyright holder or licensee to want to limit content streaming geographically and facilitation of this practice through geolocation is a logical step. What is not a logical step is turning what would otherwise be authorized access into a violation of § 1201 simply because the user, for any one of a number of reasons, has chosen to disguise their true location. Those users who knowingly obscure their IP addresses purely to gain access to content they know is restricted by location may indeed run afoul of § 1201(a), but not all users who evade geolocation are doing so for this reason. A user may access a remote machine for work or be attempting to avoid the restrictions of a repressive regime; in these cases, and others like them, the goals of § 1201(a) are not served by imposing liability. Section 1201(i) provides that where the information collected as part of the control of access is considered PII, the user circumventing the tool is not liable unless the content provider notifies the user of this data's collection. Because IP addresses provide significant data as to the location and potential identity of users, they should be considered PII for this purpose. In addition, § 1201 was passed to bring the U.S. into compliance with its treaty obligations. Other parties to the WIPO Treaty, such as the EU, have not taken the approach embraced by the Ninth Circuit. The approaches taken in the EU and by the Federal Circuit in the U.S. would generally not create liability for geolocation evasion and these are the approaches that should be followed.