THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

BLOCKING AD BLOCKERS

TYLER BARBACOVI

ABSTRACT

The prevalence of ad blocking software (software that prevents the loading of web based advertisements) is a growing problem for website owners and content creators who rely on advertising revenue to earn money. While the number of ad block users continues to increase, there has thus far been no significant legal challenge to ad blocking in the United States. This comment examines how a website owner, through a combination of technological improvements and the anti-circumvention provisions of the Digital Millennium Copyright Act, could successfully raise a legal challenge against the purveyors of ad blocking software.

Cite as Tyler Barbacovi, *Blocking Ad Blockers*, 16 J. MARSHALL REV. INTELL. PROP. L. 272 (2017).

BLOCKING AD BLOCKERS

TYLER BARBACOVI

BLOCKING AD BLOCKERS

TYLER BARBACOVI*

I. INTRODUCTION

Ad filtering software ("AFS")[1] is costing the advertising industry billions of dollars each year in lost revenue. Advertisers lost an estimated $22 billion in 2015 alone.[2] With 198 million users already using AFS, and new users signing up daily, website owners need a way to ensure that their platforms will remain viable in the face of AFS.[3]

While most browsers have some kind of limited ad filtering capabilities, like pop-up blockers, AFS typically refers to software which prevents advertisements from appearing on webpages themselves (e.g. banner ads, Flash advertisements, or the commercials that appear prior to YouTube videos). AFS is typically installed via a browser extension, or plug-in. Popular AFS includes: AdBlock, Adblock Plus, and µBlock Origin.

Most websites do not charge for accessing their content, relying on advertising revenue to make money. When an end user uses AFS, the advertisements, which normally appear on a webpage, are prevented from loading. For example, an end user with Adblock Plus enabled will not see any of the advertisements that appear prior to the video. While there are some legitimate reasons for using AFS beyond simply wishing to avoid bothersome advertisements, webpages rely on advertising revenue to earn a profit and fund the creation of their content.[4] If everyone were to use AFS,

---

* © Tyler Barbacovi 2017. Candidate for Juris Doctor, The John Marshall Law School, 2017; Bachelor of Arts Double Major in Philosophy and Politics, New York University, 2014. I would like to thank the staff and editors of The Review of Intellectual Property Law for all the hard work they do in putting this publication together. I would also like to thank Telly Nakos, Professor Steven Wiser, and Professor William Ford for everything they have done for me during my time at law school

[1] More commonly known as ad blocking software, or ad blockers. Because this comment will reference specific AFS, like Adblock Plus, I have elected to use the less commonly used term to avoid confusion.

[2] Elizabeth Morse, *Ad-Blocking Software Will Cost the Ad Industry $22 Billion This Year*, WALL ST. J.: DIGITS (Aug. 10, 2015, 6:28 PM), http://blogs.wsj.com/digits/2015/08/10/ad-blocking-software-will-cost-the-ad-industry-22-billion-this-year/. Revenue loss due to AFS rose 41% between 2014 and 2015. Approximately one third of all internet users now use some kind of AFS. This poses a significant threat to the viability of many web platforms, most of which make their content freely available to the end users.

[3] PageFair, *The Cost of Ad Blocking: PageFair and Adobe 2015 Ad Blocking Report*, PAGEFAIR at 4, http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf. PageFair is a company owned by Adobe which provides anti-AFS services. Much of the data on the effects of AFS comes from their research, and while their potential bias must be considered, sources like the Wall Street Journal, and Fortune magazine have cited their studies. While PageFair seeks to help website owners reduce the amount of advertisements being blocked on their page, their service is not free. Therefore, even if PageFair is successful content creators are only getting a portion of the advertising revenue they should. A better solution would be to stop the use of AFS altogether.

[4] PageFair, *Adblocking Goes Mainstream: PageFair and Adobe 2015 Ad Blocking Report*, PAGEFAIR at 10, https://downloads.pagefair.com/wp-content/uploads/2016/05/Adblocking-Goes-Mainstream.pdf (finding that surveyed AFS users blocked ads to improve performance and protect their privacy); *see also* Stephanie Molt, *Online Advertising More Likely to Spread Malware Than Porn*, PC MAGAZINE (Feb. 1, 2013, 12:22 PM), http://www.pcmag.com/article2/0,2817,2415009,00.asp

websites that rely primarily on ad revenue would either have to find a new means of making money, or shut down.

A. Reasons for Using AFS

There are a number of benefits of using AFS beyond simply avoiding advertisements: loading times for webpages are reduced, battery life increases, and data usage is reduced when browsing on a metered connection.[5] Most importantly, using AFS can protect end users' personal information, and serves as a first line of defense against malware.[6]

Website owners long ago lost the goodwill of users who employ AFS. Most people who use AFS realize that the content they are viewing costs something to create, and would be willing to support content creators who exercise discretion.[7] That being said, it is difficult to win back a previous user who has lost their trust.

On the other hand, AFS companies may not be the stalwart champions of the people they initially presented themselves to be. While many AFS company philosophies talk about protecting end users from invasive and malignant advertisements, Adblock Plus' white listing program has brought that into question. The default settings of Adblock Plus allows a list of pages with acceptable

---

(finding that advertisements were more likely to contain malware than pornography). AFS is frequently used to protect the end user's privacy and can be used to stop malware ridden advertisements. Additionally, many of the users who do wish to block ads only wish to block intrusive or annoying ads. Video advertisements which play sound, pop ups, and pop ins (where a notification if rendered on the page itself rather than in a separate window or tab) are seen as particularly onerous and can drive users to install AFS. Advertisers and content creators should take into consideration how these advertising practices effect their respective brands in the long term.

[5] Trevor Timm, *What Media Companies Don't Want You to Know About Ad Blockers*, COLUMBIA JOURNALISM REVIEW (Jun. 29, 2016), http://www.cjr.org/opinion/ad_blockers_malware_new_york_times.php.

[6] *See id.* (reporting that The New York Times, AOL, and BBC had their ad networks hacked resulting in advertisements attempting to install ransomware on users' computers); Alex Hern, *Major Sites Including New York Times and BBC Hit by "Ransomware" Malvertising*, THE GUARDIAN (Mar. 16, 2016), https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising (describing how ransomware uses ads to infect users' computers, encrypt their data, and sell them the key using bitcoin); Jérôme Segura, *Large Angler Malvertising Campaign Hits Top Publishers*, MALWAREBYTES (Mar. 15, 2016), https://blog.malwarebytes.com/threat-analysis/2016/03/large-angler-malvertising-campaign-hits-top-publishers/ (detailing the attack which infected various ad networks including Google). *See also* Don Reisinger, *Porn Sites: Safer Than News Sites?*, PC MAG (May 23, 2016, 5:52 PM), http://www.pcmag.com/news/344680/porn-sites-safer-than-news-sites (reporting that news sites on average track more user data than other websites, including pornographic websites).

[7] *See* Lewis DVorkin, *Inside Forbes: Our Ad Block Test Stirs Up Emotions, Then Brings Learnings and New Data*, FORBES (Jan. 14, 2016), http://www.forbes.com/sites/lewisdvorkin/2016/01/14/inside-forbes-our-ad-block-test-stirs-up-emotions-then-brings-learnings-and-new-data-2/#136a895b2cae. 44% of users who encountered Forbes' ad-wall turned off their AFS. Furthermore, users stayed on pages longer after Forbes implemented their "Ad-Light" webpage.

advertisements to reach users unfiltered.[8] While many smaller pages are added to this list free of charge, larger webpages must pay to be included.[9] This practice has been compared, perhaps not unfairly, to an extortion racket.[10] Eyeo, the company that owns Adblock Plus, is registered as a for-profit company.[11]

Additionally, website owners and advertising networks need to protect their readers from malware hiding in their advertisements. Advertisements on top news sites have repeatedly been used to distribute malware.[12]

Another major problem with advertisements is that they frequently include trackers which record personal information.[13] Separate anti-tracking applications exist to prevent users from being tracked, but many AFS have begun implementing features like this as well.

B. Attempts to Solve the AFS Problem Not Been Effective

Despite the tremendous costs to their respective industries, website owners and advertisers have been unable to find an effective solution to this problem. Some content creators and website owners have been able to find success with subscription models where users pay a recurring fee to access their content (e.g. Netflix, Hulu, and eHarmony). However, this is simply not a viable option for many websites as end users are unwilling to pay for their content.[14] Other websites have started asking for

---

[8] ABOUT ADBLOCK PLUS, https://adblockplus.org/en/about#monetization (last visited Jul. 1, 2016). "Adblock Plus users have the option to display ads that are on the Acceptable Ads list or to disable the Acceptable Ads feature and browse completely ad-free." *Id.*

[9] *Id.* "Larger entities pay a licensing fee for the whitelisting services requested and provided to them (90% of the licenses are granted for free, to smaller entities)."

[10] Lisa Vaas, *Former Googler Fights Adblockers with Adblocker Blocker*, NAKED SECURITY (Jun. 19, 2015), https://nakedsecurity.sophos.com/2015/06/19/former-googler-fights-adblockers-with-adblocker-blocker/. On AFS, Ben Barokas CEO and founder of Sourcepoint said, "It's blackmail. It's extortion. It's not fair." *Id.*

[11] Robin Wauters, *A Look Inside Eyeo, the Company Behind Ad-Blocking Software Phenomenon Adblock Plus*, TECH.EU (Sep. 24, 2014), http://tech.eu/features/2614/eyeo-profile-adblock-plus/. Eyeo is a German for profit company responsible for Adblock Plus. The company currently generates much of its revenue from its "acceptable ads" program.

[12] *See* Trevor Timm, *What Media Companies Don't Want You to Know About Ad Blockers*, COLUMBIA JOURNALISM REVIEW (Jun. 29, 2016), http://www.cjr.org/opinion/ad_blockers_malware_new_york_times.php; Alex Hern, *Major Sites Including New York Times and BBC Hit by "Ransomware" Malvertising*, THE GUARDIAN (Mar. 16, 2016), https:// www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising; Jérôme Segura, *Large Angler Malvertising Campaign Hits Top Publishers*, MALWAREBYTES (Mar. 15, 2016), https://blog.malwarebytes.com/threat-analysis/2016/03/large-angler-malvertising-campaign-hits-top-publishers/. Advertisements frequently contain malware, some of which can be quite serious, like the ransom ware that was the focus of this attack.

[13] *See* Don Reisinger, *Porn Sites: Safer Than News Sites?*, PC MAG (May 23, 2016), http://www.pcmag.com/news/344680/porn-sites-safer-than-news-sites.

[14] Nic Newman, *Executive Summary and Key Findings of the 2015 Report*, DIGITAL NEWS REPORT (2015), http://www.digitalnewsreport.org/survey/2015/executive-summary-and-key-findings-2015. While there is some content for which users are willing to pay a subscription fee like Hulu, Netflix, or Amazon Prime, end users are not willing to pay for all content. The Digital News Report survey conducted by Reuters found that 67% percent of American end users would never purchase an

donations or requesting that end users turn off their AFS. While some platforms and content creators have found success with this model (e.g. Wikipedia, and Reddit) for most this is an ineffective solution.[15] In an attempt to stem the tide of AFS, website owners have turned to technological solutions. Companies like Sourcepoint and PageFair offer to create advertisements that are undetectable to AFS.[16] While this strategy has had some success, it is costly and quickly turns into a cat and mouse game.[17] Thus far, no legal action has been taken against any major AFS company in the United States.[18]

C. The Rise of Ad-Walls

Recently, a new technological development has occurred that may spell the end for AFS. In December, 2015 Forbes added a feature to their website that detects when

---

online news subscription no matter what the price, and that the average price an American user would be willing to pay is $8.50 a year. *Id.* This is hardly a viable model. *But see* Sydney Ember, *New York Times Co. Reports Loss as Digital Subscriptions Grow*, THE NEW YORK TIMES (May 3, 2016), http://www.nytimes.com/2016/05/04/business/media/new-york-times-co-q1-earnings.html (reporting an increase in subscribers for the digital version of The New York Times).

[15] *See* The PageFair Team, *Introducing PageFair Ads,* PAGEFAIR (Apr. 8, 2014), https://blog.pagefair.com/2014/introducing-pagefair-ads//; *but see Allowing acceptable ads in Adblock Plus*, ADBLOCK PLUS, https://adblockplus.org/acceptable-ads#criteria (finding that 75% of Adblock Plus users would be willing to see reasonable ads). Only three users in a million will donate to a website soliciting donations. While asking users to not use AFS only results in .33% of users actually turning of their AFS, and a third of those will switch it back on. However, programs like Adblock Plus' (a popular AFS) white listing feature seem to have met with support. Essentially how the white listing feature works is that websites which Adblock Plus finds use advertisements in a reasonable manner will be placed on its white list. By default, advertisements from that website will not be filtered. However, end users can turn this feature off if they wish and block all advertisements. While this seems like a reasonable compromise, the service is only free for smaller companies. Larger websites must pay for this service, essentially having their advertising revenue held ransom. While some of this fee must certainly go to cover their operating costs, Eyeo, Ad Block Plus' parent company, is a for profit corporation with Ad Block Plus as their flagship product. If the program is successful, website owners are still splitting the pot. Additionally, while donations may work for some content creators like Wikipedia, Reddit, and Patreon it is not a viable solution for most companies.

[16] Similar companies include Yavli, and SecretMedia.

[17] Ania Nussbaum, *Ad Blockers, Internet Advertisers Play Cat and Mouse,* WALL ST. J. (Jul. 16, 2015), http://www.wsj.com/articles/ad-blockers-internet-advertisers-play-cat-and-mouse-1437046675. Whenever an ad becomes unfilterable, the AFS companies seek to improve their filters and are often successful. This leads to the website improving their advertisements, and the cycle repeats itself. The development costs to make AFS proof advertisements, and the uphill battle makes this solution untenable. Also, the advertising networks are often outnumbered. Not every filter works the same, and what may get past one might not get past all AFS. Additionally, most AFS are open source programs, which means that multiple users can work together to stop advertisements from appearing on that page.

[18] David Meyer, *Major Ad-Blocker Suffers Defeat Over Business Model*, FORTUNE (Jun. 24, 2016), http://fortune.com/2016/06/24/adblock-plus-axel-springer/. While there has been no significant case regarding AFS in U.S. courts, Eyeo, the parent company of Ad Block Plus was sued by Axel Springer, the parent company of Business Insider, Bild, and Die Welt for breaching German unfair competition laws. In a ruling from the Cologne higher regional court, Adblock Plus itself was found not to be in violation of German law, but Adblock Plus' acceptable ads feature was found to violate German unfair competition law. Eyeo has appealed to the Germany's supreme court.

users are using AFS and denies them access until their AFS is turned off (hereafter referred to as "ad-wall"). However, users swiftly found a way around this, allowing them to continue using their AFS on the site.[19] It is a good thing too because in January, 2016 advertisements on Forbes were found to contain malware.[20] Forbes' ad-wall turned out to be easily circumvented, and implored users to turn off their AFS only to serve them malware-ridden advertisements. Without even realizing it, website owners may have won the war against AFS.[21]

Websites which use ad-walls have created a technology that restricts access to their webpage. AFS companies have two ways to respond. Either they can do nothing, in which case the ad-wall effectively stops users with AFS from accessing their webpage; or they can improve to their AFS in order to breach the ad-wall. The Digital Millennium Copyright Act ("DMCA") includes a provision which makes it illegal to circumvent technological measures designed to protect copyrightable material.[22] If an AFS company were to breach a website's ad-wall, it would be in violation of the DMCA's anti-circumvention provisions. Therefore, a website owner could effectively protect their content from AFS by implementing an ad-wall, and diligently prosecuting claims against any AFS company who breaches that wall.[23]

This comment will rely on a hypothetical scenario in which a website creates an effective ad-wall. Then an AFS improves their program and breaches the ad-wall.[24]

---

[19] *How to use Forbes.com with Adblock?*, REDDIT (Dec. 19, 2015), https://www.reddit.com/r/Adblock/comments/3zkj1a/how_to_bypass_forbes_magazine_on_adblock/. Shortly after Forbes implemented their ad-wall internet users had already found a way to bypass the ad-wall. While these actions would not create a cause of action against the AFS themselves, it is important to remember that many AFS are open source, and solutions from the community may be adopted by the platform itself. Also, it is presumable that websites will continue to develop ad-walls that require more than three lines of code to break.

[20] Violet Blue, *You Say Advertising, I Say Block That Malware*, ENGADGET (Jan. 08, 2016), https://www.engadget.com/2016/01/08/you-say-advertising-i-say-block-that-malware/. Shortly after Forbes' ad-wall was implemented, their advertisements began distributing malware to end users' computers. This does not exactly bolster confidence in advertisers, or website owners.

[21] *How To Bypass Websites that Block "AdBlock"* (e.g. Forbes), TECH NEWS REPORTER (Dec. 19, 2015), http://technewsreporter.blogspot.com/2015/12/how-to-bypass-websites-that-block-ad.html; *see also* Forbes™ Splash Screen Bypass, https://chrome.google.com/webstore/detail/forbes-splash-screen-bypa/gjiddhnfkgbnnhbghaacfofkopmgleij?hl=en (a browser extension designed to bypass Forbes' anti-AFS ad-wall). Shortly after Forbes implemented its ad-wall technology, users began to find ways of circumventing it.

[22] 17 U.S.C. § 1201(a-b) (West 2012). The anti-circumvention provisions create a separate cause of action for circumventing an access protection measure, and trafficking in access and copy protection circumvention technology. This is advantageous because, copyright owners can pursue not only end users, but those distributing the AFS.

[23] While a legal solution is a drastic step, it is clear that attempts to find technological and market solutions to the growing problem of lost advertising revenue have not been completely successful. Additionally, while other legal theories have been proposed, such as copyright infringement and tortious interference with contract, no successful legal challenge has been made against a AFS in the United States. Jordan L. Walbesser, *Blocking Advertisement Blocking: The War Over Internet Advertising and the Effect on Intellectual Property*, 23 No. 1 INTELL. PROP. & TECH. L.J. 19, 21-22 (2011) (arguing that AFS is a copyright infringement); Andrew Saluke, *Ad-Blocking Software As Third-Party Tortious Interference with Advertising Contracts*, 7 FLA. ST. U. BUS. REV. 87 (2008) (arguing that AFS is tortious interference with contract).

[24] A WEBSITE IS TELLING ME TO DISABLE ADBLOCK BEFORE IT WILL SHOW CONTENT, https://help.getadblock.com/support/solutions/articles/6000082125-a-website-is-telling-me-to-disable-adblock-before-it-will-show-content (last visited Aug. 6, 2016); and REPORT AN ISSUE,

Part I provides the relevant anti-circumvention provisions of the DMCA, and case law regarding the elements of anti-circumvention claims. Part II examines how likely the website owner would be to succeed on an anti-circumvention claim given the current state of the law. Part III discusses how website owners can take steps to protect themselves against AFS by developing ad-wall technology, as well as extra-legal considerations that website owners should consider when contemplating legal action.

II. BACKGROUND

A. Anti-Circumvention Provisions

The DMCA's anti-circumvention provisions are codified at 17 U.S.C. § 1201. There are three ways in which a potential user can violate the provisions of this statute: circumventing an access protection, trafficking in technology which circumvents an access protection, and trafficking in technology which circumvents a copy protection.[25]

Circumventing an access protection has four elements: "(1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, . . . [(3)] without authorization, in a manner that [(4)] infringes or facilitates infringing a right protected by the Copyright Act . . . ."[26]

Trafficking in technology which circumvents an access protection has six elements:

> (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[27]

---

https://adblockplus.org/bugs (last visited Aug. 6, 2016). AdBlock, and Adblock Plus, encourage users to report websites that request users turn off AFS, presumably in order to circumvent these problems.

[25] 17 U.S.C. § 1201 (a)(1) (circumventing an access protection measure); 17 U.S.C. § 1201 (a)(2) (trafficking in a technology which circumvents an access protection measure); 17 U.S.C. § 1201 (b) (trafficking in a technology which circumvents a copy protection measure).

[26] *Id.* § 1201(a)(1)-(34); *See also* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004); 17 U.S.C. § 1201(a)(1) (The *Chamberlain* court originally defined the elements of a 17 U.S.C. § 1201(a)(2) cause of action. Because all elements of a § 1201(a)(1) claim are included in a § 1201(a)(2) claim, elements were deleted from the *Chamberlain* to create a definition for a circumventing an access provision.).

[27] *Chamberlain Group*, 381 F.3d at 1203. The court clearly defined the elements for trafficking in technology which circumvents an access provision.

It should be noted that there is a circuit split regarding the interpretation of these two violations, so it may not be necessary to demonstrate that the access circumvention facilitates infringement of the plaintiff's copyright. In order to be thorough, however, it will be included in the analysis portion of this comment.[28]

The statute also defines circumventing an access protection as "descrambl[ing] a scrambled work, decrypt[ing] an encrypted work, or otherwise avoid[ing], bypass[ing], remov[ing], deactivat[ing], or impair[ing] a technological measure, without the authority of the copyright owner[.]"[29] Additionally, an access protection is effective when "in the ordinary course of its operation, [it] requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[30] These definitions apply to both circumventing an access protection, and trafficking in technology which circumvents an access protection.

Trafficking in technology which circumvents a copy protection has six elements:

> (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now [copy or otherwise exercise rights of the copyright holder] (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[31]

The statute defines circumvention of a copy protection as "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure . . . ."[32] Additionally, a copy protection measure "effectively protects a right of a copyright owner . . . [when] in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title."[33]

Essentially, the differences in these three violations can easily be broken down. It is a violation of the DMCA to circumvent an access protection. It is also a violation

---

[28] *Id.* at 1195 (the Federal Circuit has held that a § 1201 violation "applies only to circumventions reasonably related to protected rights."); MDY Industries, LLC v. Blizzard Ent., Inc., 629 F.3d 928, 952 (9th Cir. 2010), as amended on denial of reh'g (Feb. 17, 2011), opinion amended and superseded on denial of reh'g, 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011) (the Ninth Circuit has held that there is no infringement nexus requirement). The circuit split is ultimately inconsequential to this analysis, because the activity which AFS users practice will ultimately be shown to constitute a copyright infringement.

[29] 17 U.S.C. § 1201(a)(3)(A).

[30] *Id.* § 1201(a)(3)(B). Courts have held that protection can still be effective even if a circumvention is readily available. Analogizing a technological protection measure to a lock, a district court found that even if it is "easy to find skeleton keys on the black market, a deadbolt is [still] an effective lock to a door." *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004).

[31] 17 U.S.C. § 1201(b)(1); *Chamberlain Group*, 381 F.3d at 1203; The *Chamberlain* court originally defined the elements of a 17 U.S.C. § 1201(a)(2) cause of action. Because the elements of a § 1201(b)(1) claim are similar to the elements a § 1201(a)(2) claim, element (3) was modified to create a definition for trafficking in technology which circumvents a copy protection.

[32] 17 U.S.C. § 1201(b)(2)(A).

[33] *Id.* § 1201(b)(2)(B) (internal quotations omitted).

to traffic in technology which circumvents an access protection or a copy protection. However, it is not a violation to merely circumvent a copy protection.

B. General Statutory Elements

First, in order to succeed on any anti-circumvention cause of action, a plaintiff must demonstrate ownership of a valid copyright. Website codes has been granted copyright protection and can be registered with the U.S. Copyright Office.[34]

Second, a plaintiff must also show that the work was effectively controlled by a technological measure. One example of a technological control measure is a CAPTCHA, a technology which is used to verify that a website is being used by a human and not a robot. This typically works by displaying a distorted image of text and requiring the user to input the text into a field. CAPTCHA is used to detect the use of automated programs on a webpage. Because CAPTCHA requires the application of information to access copyrighted material, it has been found to constitute an access control measure.[35] Further, CAPTCHAs are also a copy protection because they prevent the unauthorized use of automated programs on webpages.[36] Additionally, a program which scans for the absence of cheats or bots in an online game is also considered to be an access control measure.[37]

Third, a plaintiff must also show that there was unauthorized access. Defining what behavior is and is not permitted in the Terms of Use can help define unauthorized access.[38] Additionally, courts have held that implementing an automated protection system which refuses entry to certain users can itself define what is and is not authorized, since the systems were put in place by the website owner.[39]

---

[34] Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1104 (C.D. Cal. 2007). For the sake of this analysis, the plaintiff is presumed to have a website which is eligible for copyright protection, obviously if a website owner does not have a website which can achieve protection the analysis would be different.

[35] *Id.* at 1112.

[36] *Id.* Because the CAPTCHA code prevented the unauthorized access of automated users, and user which did get through violated the terms of use for Ticketmaster's website and therefore made an unauthorized copy of the page.

[37] MDY Industries, LLC v. Blizzard Ent., Inc., 629 F.3d 928, 954 (9th Cir. 2010), as amended on denial of reh'g (Feb. 17, 2011), opinion amended and superseded on denial of reh'g, 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011). Here the court found that Blizzard's Warden program which scanned the user's computer for cheats and bots constituted an access protection measure because, this constituted a process or treatment under 17 U.S.C. § 1201(a)(3). This is clearly analogous to the way in which ad-wall protections scan for AFS and deny access to users who do not turn off their filters.

[38] *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1110; *MDY Industries*, 629 F.3d at 939. In these cases, the courts found that the terms of use on the website defined what was and was not an authorized use, effectively creating a license agreement. Because this analysis is examining an anti-circumvention provision in the light most favorable to a potential plaintiff, it is stipulated in the fact pattern that the plaintiff has made it a term of use that the user shall not use AFS on their website. Ideally these terms of use will be displayed on a "splash page" which informs blocked users to turn off their AFS. That way the end users are clearly made aware of the terms before they enter the website.

[39] *MDY Industries*, 629 F.3d at 954. The court found that by simply implementing a gatekeeper technology, in this case "Warden", which scanned for cheaters in the World of Warcraft online game, was enough to put the user on notice that the activity is unauthorized. The reasoning is that an

Finally, a plaintiff may have to show that the circumvention either infringes or facilitates infringement of their copyrighted material. One of the rights granted to a copyright owner is the right to create copies of the work.[40] In order for a valid copyright to exist, the work must be fixed in a tangible medium of expression for more than a transitory duration.[41] Merely loading a webpage without authorization can constitute "fixation" in terms of copyright infringement.[42] Copying a copyrighted work in the Random Access Memory ("RAM") of a computer is sufficient to constitute copying.[43] Because webpages can be copyrighted and opening a webpage typically creates a copy of the website in the RAM of a computer system, simply viewing a webpage can constitute an infringement if the viewing is unauthorized.

C. Trafficking Elements

To succeed on either of the trafficking causes of action, a plaintiff must demonstrate that the circumvention technology had been made available to third parties. The courts have held that trafficking in circumvention provisions can be interpreted broadly; even linking to a website known to contain circumvention codes has been found to constitute trafficking.[44] Likewise, distributing and selling circumvention tools is also considered trafficking.[45]

---

automated system which prevents cheaters from logging on to World of Warcraft's servers is like a wall or locked door. They in and of themselves inform those who interact with them that the area beyond is unauthorized.

[40] 17 U.S.C. § 106(1) (2012). The right to make copies is an exclusive right which the owner has in the copyrighted material. Unless there is a defense like fair use, making an unauthorized copy is considered to be an infringement. Because the viability of an anti-circumvention claim may depend on whether or not the circumvention constitutes an infringement, a fair use defense may be important to this element. *See* PAGEFAIR *supra* note 15 and accompanying text. That being said, it would have to be shown that the AFS was primarily designed not to infringe.

[41] 17 U.S.C. § 101 (2012).

[42] *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1106. In this case, the website was being loaded by a user who had violated the terms of use which made the use unauthorized.

[43] MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993). Random Access Memory is volatile storage in which files can be temporarily loaded to the computer for use. While this data is constantly changing and permanent copies are typically stored on the hard drive of a computer, websites are saved temporarily to the RAM and are still visible to users. This is how people are able to browse webpages. The important thing is that the webpage is fixed long enough to be perceived and interacted with. Thus, a copy is created, and if it is unauthorized, then that copy would constitute an infringement of the owner's copyright.

[44] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 456 (2d Cir. 2001). (finding that simply linking to another website where anti circumvention technology could be found was enough to constitute trafficking). Simply linking to webpage normally would not constitute trafficking, however, under extreme circumstances it can.

[45] *See, e.g.*, U.S. v. Silvius, 559 Fed. Appx. 490 (6th Cir. 2014) (unpublished), *as amended* (Apr. 7, 2014); U.S. v. Reichert, 747 F.3d 445 (6th Cir. 2014). Trafficking is generally considered to include providing the circumvention technology to another. If the plaintiff is successful on their claim they could potentially pursue action against anyone hosting the AFS. In the real world AFS are frequently hosted by web browsers, meaning real world clients could potentially be dealing with Google, Mozilla, and Apple. This would be desirable as it has the potential of bringing the most relief.

If a plaintiff is successfully granted an injunction against the owners and distributors of an AFS Program to prevent the distribution of the AFS, then the plaintiff will have effectively prevented that AFS from being used on their website.[46] By using an ad-wall to prevent the use of AFS on their website and by successfully suing for injunctive relief when one of the blocked AFS is improved to circumvent the ad-wall, the plaintiff can ensure that AFS is not used on their webpage.

III. ANALYSIS

For the sake of analysis, it is presupposed that the plaintiff has a valid copyright to the content and the source code of its webpage. For most website owners satisfying this element is problematic.[47]

A. Is an Ad-Wall an Effective Protection Measure?

The first consideration is whether the plaintiff has a technological measure which effectively controls access, and if so, does the improved AFS circumvent that protection? While Ad-wall technologies are designed to get the user to view ads, and programs like Warden, or CAPTCHA are designed to stop the use of automated bots on webpages, both technologies serve the same purpose. They detect and stop unauthorized use of third party technologies on webpages. In this case plaintiff's ad-wall initially stopped the AFS from accessing the plaintiff's webpage. Ad-wall technologies which detect and block users who have installed AFS are substantially similar to the Warden technology used by Blizzard, the developer of the World of Warcraft video game to detect cheaters in the game.[48] In Blizzard's case, end users began to use a bot called Glider to automatically play through the games early stages.[49] Blizzard became aware of Glider and in response created Warden, a technology designed to block Glider users from connecting to the World of Warcraft servers.[50]

---

[46] 17 U.S.C. § 1203(b)(1) (2012).

[47] *See Ticketmaster L.L.C.*, 507 F. Supp. at 1111 (holding that the Ticketmaster website is copyrightable). Theoretically, if a webpage uses open source code and hosts only content in the public domain, the website might not contain any copyrightable material. For most website owners this should not be a problem, and the website's code and/or content should be eligible at least in part for copyright protection.

[48] *MDY Industries*, 629 F.3d at 936.

[49] *Id.* at 935. In World of Warcraft, characters complete quests to level up and gain gear. Glider was designed to automate the player's progression through the early levels in order to help reach the end of the game more quickly. Many players view the game's end game content (the content available to players who have attained the maximum level) to be the most desirable and fun portion to play, hence, the desire to automate the earlier levels. Additionally, the game allows each player to have multiple characters, thereby, a player who has already attained maximum level with their initial character may desire to quickly level up a second character.

[50] *Id.* at 936.

Warden functioned by scanning the computer's RAM for Glider and then permitting a user access to the servers if the computer was found to be free of Glider.[51]

In the case of ad-wall technology, the website scans the user's computer for AFS. If it is detected, the user is then directed to a splash page which informs the user that the use of AFS is prohibited and instructs the user to disable it in order to gain access to the website. If the software is not detected, the end user is then allowed to connect to the server which hosts the copyrighted material. If, however, banned software is detected, then the end user is not permitted to access the content. The two technologies effectively do the same thing, albeit for dissimilar purposes.

Initially, Blizzard's Warden was successful.[52] It managed to detect most Glider users and prevent them from accessing the game while using the bot.[53] The developer of Glider then modified the bot, making it more difficult to be detected by Warden.[54] Glider was reconfigured so that it did not load until after the initial scan was completed.[55] In our hypothetical scenario, the offending AFS was modified so that plaintiff's ad-wall technology no longer detected the AFS, thus enabling users to access the plaintiff's webpage while still using the modified AFS.[56]

In each instance, the technology was modified in order to avoid the detection of a technological protection measure. Therefore, the modified AFS constitutes a circumvention of an access protection.[57]

While ad-wall technology currently relies on actively scanning the end user's computer, the technology could theoretically also take a form similar to CAPTCHA, where the end user is required to answer a simple question regarding the advertisement to access the content.[58] If the end user has blocked the advertisement they will not be able to answer the question.

---

[51] *Id.* at 942. Warden also intermittently scanned the RAM of users who had connected to World of Warcraft's servers for code which indicated that Glider was in use. If detected, the user would be booted from the game's servers. The court held that this also constituted an access prevention measure. So, theoretically, a technology which revoked access to a webpage upon detecting that advertisements had failed to load could also constitute a viable access protection measure.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *How To Bypass Websites that Block "AdBlock"* (e.g. Forbes), TECH NEWS REPORTER (Dec. 19, 2015), http://technewsreporter.blogspot.com/2015/12/how-to-bypass-websites-that-block-ad.html. At the time of the writing of this comment (April-October 2016), Forbes is one of the only websites utilizing such technology, and thus far none of the blocked AFS have circumvented it. However, third parties have found a variety of work arounds. These workarounds effectively function by blocking outbound information from the user's computer to Forbes, preventing Forbes' ad-wall from detecting that the user is using Ad Block Plus.

[57] *MDY Industries*, 629 F.3d at 954 (because Warden was initially effective at stopping Glider, it was deemed to be an effective protection measure).

[58] Ticketmaster L.L.C., 507 F. Supp. 2d at 1112 (finding CAPTCHA to be an access protection measure). Filters which require the user to enter a word or phrase embedded in the advertisement, have the added benefit of functioning against any AFS; while technology which relies on detecting AFS is only effective against the AFS it is designed to detect. Additionally, such measures would force the user to engage with the advertisement. On the other hand, these methods may be seen as overly pushy. End users may be willing to tolerate CAPTCHA as a security measure, but may dislike similar technology being used to quiz them on their commercials.

B. Was the Website Viewed Without Authorization?

Next the plaintiff must show that a user who viewed the website while using the improved AFS accessed the website without authorization. Let us suppose that the plaintiff has included text in the end user license agreement ("EULA") and on the splash page specifying that the use of AFS on their web page is prohibited. This would put the plaintiff in a desirable position since a website's terms of use can be used to determine what is considered authorized and unauthorized access to that website.[59] When Ticketmaster issued the following warning in its terms of use, "[y]ou do not have permission to access this Site in any way that violates . . . these terms of use," they effectively granted consumers a license to copy their webpage in compliance with their terms.[60] As such, If the plaintiff states in the website's terms of use, that access to the site's content is conditioned on end users not using AFS, they will effectively do the same thing.[61]

While Ticketmaster's terms of use prohibited bots from being used on its webpage, the underlying principle is the same as the plaintiff's prohibition on AFS. In each case, the terms of use prohibit the use of certain unauthorized software on their websites.[62]

While it is desirable for website owners to include terms of use which prohibit AFS by clearly defining the use of AFS as unauthorized behavior, the mere existence of the ad-wall technology is likely sufficient.[63] Warden was found to operate within the authority of Blizzard, the automated system dictated the terms of use simply by being implemented.[64] Having an ad-wall is enough to make the circumvention of the ad-wall unauthorized.[65]

---

[59] *Id.* at 1108 (finding Ticketmaster's terms of use to grant users a non-exclusive license to copy and view the Ticketmaster website in accordance with the terms of service).

[60] *Id.*

[61] *See also* Nguyen v. Barnes & Noble, Inc., 8:12-CV-0812-JST RNB, 2012 WL 3711081, at *4 (C.D. Cal. Aug. 28, 2012), aff'd, 763 F.3d 1171 (9th Cir. 2014) (emphasizing the importance of the placement of terms of service has on their effectiveness). The terms of Barnes and Noble's "browsewrap" agreement (which appeared on the bottom left of its webpage) were found to be unenforceable. The court distinguished Barnes and Noble's "browsewrap" agreement from Ticketmaster's "clickwrap" agreement. Website owners should take practical steps to ensure that end users are aware of the terms of use, like including their ad block policy on a splash page, or placing notifications in the space where ads normally appear, so that users are put on notice when those advertisements are blocked.

[62] *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1108. Additionally, the terms of use in each case are definite enough, so that they are not considered to be unenforceably vague.

[63] *MDY Industries*, 629 F.3d at 954.

[64] *Id.* (finding that because Warden was implemented by Blizzard, it could be reasonably inferred that Blizzard did not approve the use of bots on their servers).

[65] Terms of use function like a no trespassing sign. They explicitly dictate what is and is not unauthorized access. While technology like ad-walls or Warden function like a fence or locked door. While not explicitly declaring that entrance is not permitted, it may be implied by these things very existence that one is not permitted to enter.

C. Does the AFS Facilitate Infringement?

As there is currently a circuit split on this element, a plaintiff may be required to demonstrate that the access infringes or facilitates infringement of their copyright for all the anti-circumvention causes of action.[66] As discussed above, by including a prohibition against AFS in the terms of use, the website owner grants visitors to the website a non-exclusive license to make copies of their webpage, provided that the visitor does not use AFS. Visitors to the plaintiff's website create copies of the plaintiff's webpage on the RAM of their computers. In the same way that the unauthorized use of a bot on Ticketmaster's webpage was found to constitute infringement, when an end user accesses the plaintiff's website in violation of plaintiff's prohibition on AFS, that access would constitute a creation of an unauthorized copy.[67]

Ideally, a website owner will wish to bring one of the trafficking causes of action against AFS companies. This enables the owner to prevent distribution of the AFS at all levels. Currently, AFS is primarily distributed as browser extensions for web browsers.[68] For instance, Google Chrome features a storefront where users can search for extensions and apps.[69] An anti-trafficking lawsuit could potentially prevent browsers like Chrome and Firefox from distributing AFS as extensions.[70] If AFS can be removed from the various web browser extension storefronts, it would make it more difficult for AFS companies to distribute their programs.[71]

---

[66] *MDY Industries*, 629 F.3d at 948-52; *Chamberlain Group*, 381 F.3d at 1195. The Federal Circuit has held that an infringement nexus is required for anti-circumvention claims, while the 9th Circuit has held that it does not.

[67] *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1110 (holding that the use of bots in violation of Ticketmaster's terms of service constituted copyright infringement); *but see MDY Industries*, 629 F.3d at 939-42. There is also a circuit split regarding whether or not the use of bots in violation of the terms of use constitutes a violation of a license condition or a contractual provision. Fortunately, the 9th Circuit has thus far been the one to raise these concerns, and it does not require a nexus of infringement showing in DMCA anti-circumvention cases.

[68] Browser extensions are software that modifies the user's web browser by adding new features. They are typically obtained from the browser's storefront. This means that the web browser is involved in the distribution of the extensions in so far as the content is hosted on their platform.

[69] CHROME WEB STORE, https://chrome.google.com/webstore/category/apps (last visited Sep. 29, 2016).

[70] 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004). The anti-trafficking provisions of the DMCA have been broadly interpreted to include activities as varied as selling software to make unauthorized copies of DVDs. *See also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 457-58 (2d Cir. 2001). Additional activities include selling specialized microchips which allow users to play pirated video games, *see* U.S. v. Silvius, 559 Fed. Appx. 490, 492 (6th Cir. 2014) (unpublished), as amended (Apr. 7, 2014). The anti-circumvention provisions apply broadly. If the AFS is found to constitute a circumvention technology, then anyone hosting or distributing the software could be enjoined from doing so.

[71] The most determined users will likely still find ways to circumvent these protection measures, but removing them from reputable mainstream distributers will probably be enough to stop most people from utilizing AFS.

D. Was the AFS Made Available to Third Parties?

Trafficking requires that the technology is made available to third parties. This element is easily met. Millions of users use AFS, and most the software directly from their web browser.[72]

E. Is the Primary Purpose of the AFS Circumvention?

Next, the plaintiff must show that the AFS was "(i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure."[73] This is a fact specific inquiry which will depend greatly on the individual AFS in question. It is important to note that the technology need not be considered as a whole in this analysis—a single feature of a greater work may be considered independently.[74]

As a whole, an AFS is designed to block advertisements from appearing which, in and of itself is not a circumvention of an access or copy protection measure. However, when an AFS is updated to breach a website owner's ad-wall, that update is designed primarily to circumvent a technological protection measure. The overall functionality of the AFS is not impaired by the ad-wall.[75] The AFS still works on other websites.

The situation is analogous to a DVD burner. A DVD burner is not, in and of itself, illegal technology, and its primary purpose is not circumvention. If, however, DVD manufacturers place copy protections on their DVDs, circumventing them would constitute a violation of the DMCA even though the DVD burners' primary purpose is to make copies, not to circumvent.[76] The two aspects of the technology are separable such that the circumvention measure can be considered separately of the DVD burner. Does this significantly limit the utility of a DVD burner? Certainly. The same is true of AFS. The ability of AFS to block advertisements is no doubt the primary purpose. AFS functions on all webpages and it would not be practical to say that its ability to circumvent a single website's protections transforms the entirety of the software into

---

[72] PageFair, *The Cost of Ad Blocking: PageFair and Adobe 2015 Ad Blocking Report*, PAGEFAIR at 4, http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf. Hosting AFS is generally enough to satisfy the third-party requirement.

[73] *Chamberlain Group*, 381 F.3d at 1203 (finding only one of the three factors needs to be satisfied to satisfy this element).

[74] *See* RealNetworks, Inc. v. Streambox, *Inc.*, 2:99CV02070, 2000 WL 127311, at *7-10 (W.D. Wash. Jan. 18, 2000). This case involved software that downloaded streaming videos for permanent storage. The software had some non-infringing uses, such as downloading streams which the owner had permitted users to download, and converting them to other video formats. However, the software was also used to download streaming video which the video owners had explicitly marked as "not for download." The court examined the infringing portion of the technology, and found that it was separable from the legitimate portion.

[75] The non-circumvention uses of the AFS, blocking advertisements, are separable from the circumvention provisions.

[76] *See 321 Studios*, 307 F. Supp. 2d at 1098 (the court focused on a specific feature in the device and its primary purpose rather than the purpose of the device as a whole).

a circumvention measure. However, the circumvention measure is a separable feature from AFS's other functions such that it can be considered on its own.[77]

The changes made in updating the AFS to circumvent plaintiff's ad-wall serve no other purpose. Therefore, it is fair to say that that feature of the offending AFS is primarily designed to circumvent the plaintiff's protection measures (i.e. the ad-wall). Additionally, there is no other significant use for the changes made to the offending AFS. The technology has no other purpose. Obviously, it would be fortunate for a potential claimant if the AFS marketed itself as capable of circumventing anti-AFS protection measures.[78]

F. Statutory Analysis

To tie all of these elements together, a website owner should prevail against an AFS company in a suit for any of the anti-circumvention causes of action, provided the following is true: the owner's ad-wall was an initially effective against the AFS, the AFS was upgraded to circumvent the ad-wall, and the AFS was distributed to 3rd parties. When the AFS is used, the AFS circumvents the ad-wall, creating unauthorized copies of the owner's website on the accessing computer's RAM. AFS circumvented an access protection in violation of 17 U.S.C. § 1201(a)(1).[79]

Further, the AFS was distributed to third parties—it allowed third parties to also gain access to the owner's website in violation of its terms of use. The anti-circumvention features of the updated offending AFS were designed primarily, if not exclusively, to circumvent the plaintiff's ad-wall, and there is no other commercial significance to the updated offending AFS beyond its circumvention abilities. Therefore, the owner of the offending AFS is in violation of 17 U.S.C. § 1201(a)(1) for trafficking in an access protection circumvention technology.[80]

---

[77] *Cf. Ghostery*, About Us, https://www.ghostery.com/about-us/about-ghostery/. Ghostery is a browser extension which blocks websites from tracking user's personal information. Ghostery's primary purpose is to prevent trackers from monitoring users' online activity. A side effect of this browser extension is that Ghostery effectively circumvents Forbes' ad-wall technology when used in conjunction with Ad Block Plus. However, because the primary purpose of Ghostery is blocking trackers, and not to circumvent Forbes' ad-wall, Ghostery's owners are not in violation of the DMCA.

[78] For the purpose of this comment to demonstrate a best-case scenario for the proposed cause of action, the hypothetical scenario was skewed in the plaintiff's favor and references to marketing were left out of the fact pattern. This was done to demonstrate that the viability of a website owner's claim would not depend on how the AFS advertised.

[79] The viability of a circumvention of an access protection claim is not tremendous. While the claim would likely succeed, it is desirable to stomp out as much of the AFS as possible. This cause of action limits potential defendants to only those who have actually circumvented the protection. Furthermore, going after end users individually would not only be expensive, but it would likely be damaging to the website's brand. If the website owner were to go after individuals using AFS, not only would they likely stop using that webpage, the public relations backlash would likely lose the website traffic. *See* Martin Anderson, *Sites that Block Adblockers Seem to be Suffering*, THE STACK (Apr. 21, 2016), https:// thestack.com/world/2016/04/21/sites-that-block-adblockers-seem-to-be-suffering/ (demonstrating the websites who implement ad-walls tend to see a decrease in traffic).

[80] The anti-trafficking provisions are much more desirable as causes of actions, because all levels of distributors can be targeted. Additionally, some web browsers might opt not to fight a demand that the AFS be removed if the website owner had already prevailed against the AFS owner. For instance,

Additionally, because accessing the plaintiff's website necessitates that a copy of the website's code is created in the RAM of the accessing computer and the terms of use prohibit the use of AFS on the website, the offending AFS effectively creates an unauthorized, and therefore, infringing copy of the plaintiff's website. Because of this, the offending AFS is also trafficking in a technology which circumvents a copy protection under 17 U.S.C. § 1201(b).

Under the facts as described a website owner could raise a viable claim against the owner of the offending AFS for any of the three anti-circumvention causes of action. Additionally, the anti-trafficking claims could be raised against anyone who is distributing the content, including web browsers or third party websites.

IV. EXTRA-LEGAL CONSIDERATIONS & CONCLUSION

As demonstrated above, a website owner who implements ad-wall protections akin to the one used by Forbes creates a technological access protection to their copyright protectable webpage. Once in place, any updates made to the blocked AFS to get around the ad-wall constitutes a circumvention of a technological protection measure, and may be in violation of the DMCA's anti-circumvention provisions.[81] Therefore, in order to protect their webpages against AFS, website owners should invest in effective ad-wall technologies, and litigate against any AFS that circumvents their ad-walls. That being said, there are some extra-legal considerations that website owners should be aware of.

At the time of writing, ad-wall protections were not widely implemented.[82] That being said, Forbes and Wired already use ad-wall technologies and The New York Times may soon follow.[83] While ad-walls may seem like the magic bullet to finally rid

---

Google, the creator of the Chrome web browser, generates large amounts of money from advertisements. On the other hand, extensions are a valuable commodity in the browser wars, and no browser wants to be the first to drop AFS. See Richard Lawler, *AdBlock and AdBlock Plus are available for Microsoft Edge*, ENGADGET, (Jun. 07, 2015) https:// www.engadget.com/2016/05/07/adblock-adblock-plus-extensions-are-available-for-microsoft-edg/.

[81] 17 U.S.C. § 1201 (2014).

[82] *See,* Martin Anderson, *Sites that Block Adblockers Seem to be Suffering,* THE STACK (Apr. 21, 2016), https://thestack.com/world/2016/04/21/sites-that-block-adblockers-seem-to-be-suffering/ (showing that Wired, Forbes, City AM, and the German website Bild have all implemented some form of ad-wall technology); Lucia Moss, *GQ is now Blocking its Readers Running Ad Blockers*, DIGIDAY (Dec. 24, 2015), http://digiday.com/publishers/gq-now-blocking-readers-running-ad-blockers/ (showing GQ implemented an ad-wall protection); Agence France-Presse in Paris*, French News Sites Block the Adblockers Telling Readers to Uninstall or Lose Access*, THE GUARDIAN (Mar. 21, 2016), https://www.theguardian.com/media/2016/mar/22/french-news-sites-block-the-adblockers-telling-readers-to-uninstall-or-lose-access (reporting that French news sites, L'Equpie and Le Parisien implemented ad-walls). Only a handful of webpages have begun to use this technology at the time of writing this comment. Even then, after testing various combinations of AFS, I could not get the ad-wall to trigger for GQ. This seems to indicate that work-arounds may have already been implemented by AFS.

[83] Digital Content Next, *What New York Times President and CEO Mark Thompson had to say about Ad Blocking,* DIGITAL CONTENT NEXT (Jun. 6, 2016), https://digitalcontentnext.org/blog/2016/06/06/what-new-york-times-president-and-ceo-mark-thompson-had-to-say-about-ad-blocking/. ("No one who refuses to contribute to the creation of high quality journalism has the right to consume it. We are not there yet but, if we judge that it will strengthen the long-term prospects of that journalism

content creators of AFS once and for all, website owners and advertising networks would be wise to consider why AFS became so prevalent regardless of who is to blame for the current state of affairs. If website owners opt to implement ad-walls, and then proceed to use the same advertising methods that led users to install AFS in the first place, there is a decent chance that they will simply lose traffic in favor of other webpages.

A. Alienating AFS Users may be a Poor Business Decision

Website owners should consider the consequences that ad-walls have. While the current sample size is relatively small, early data seems to indicate that ad-walls may adversely affect page views.[84] Websites may lose further good will by taking steps against AFS. There is also a bit of a first mover problem inherent in deciding whether or not to implement an ad-wall. For instance, if The New York Times were to implement their own ad-wall, there is a segment of users who would simply stop using the New York Times, and get their news from another source. While this segment may seem like the last group of a people that a website would want to have as readers (they view the content without compensating the website owner), paradoxically, they may be the most desirable segment of users to advertisers.

Research suggests that many AFS users are tech-savvy millennials, a highly desirable demographic for advertisers.[85] Furthermore, because AFS users see less advertisements than other users, they are more inclined to pay attention and interact with the few advertisements that do reach them.[86] The one caveat is that these advertisements need to be respectful of these users. They cannot include trackers or be overly obnoxious.[87] Websites should do their best not to alienate these consumers. Furthermore, one of the takeaways from Forbes' experiments with an ad-wall is that end users appreciate less intrusive advertisements.[88] Visitors will spend more time on a webpage if there are fewer intrusive ads.[89] They are also more likely to "click through" and visit the advertised page.[90]

---

to prevent non-subscribers who employ ad blockers and refuse to whitelist us from reading it, we'll do it.").

[84] Martin Anderson, *Sites that Block Adblockers Seem to be Suffering,* THE STACK (Apr. 21, 2016), https://thestack.com/world/2016/04/21/sites-that-block-adblockers-seem-to-be-suffering/.

[85] Jasper Jackson, *Block ads? That Only Makes You More Attractive to Advertisers*, THE GUARDIAN (Feb. 16, 2016), https://www.theguardian.com/media/2016/feb/16/ad-blocking-advertisers.

[86] *Id.*

[87] David Barton, *Ad Block Users Are About to Become a Significant Marketing Opportunity*, PAGE FAIR (Jan. 6, 2016), https://pagefair.com/blog/2016/ad-block-users-are-about-to-become-a-significant-marketing-opportunity/.

[88] Lewis DVorkin, *Inside Forbes: Our Ad Block Test Stirs Up Emotions, Then Brings Learnings and New Data*, FORBES (Jan. 14, 2016), http://www.forbes.com/sites/lewisdvorkin/2016/01/14/inside-forbes-our-ad-block-test-stirs-up-emotions-then-brings-learnings-and-new-data-2/#136a895b2cae.

[89] *Id.*

[90] *Id.* "Click throughs" are generally considered to be the best-case scenario for an online advertiser. It indicates not only that the user has seen the advertisement, and taken notice, but that they are actively interested in learning more about the offer. Webpages also generate more ad-revenue per click through than per views.

Suppose that, after due consideration, a website owner has decided to expend the resources to implement an ad-wall. The website has also revamped its advertisements to be less intrusive and more appealing to their customers. It should still be wary of going after AFS in the legal arena.

While a DMCA cause of action has a decent chance of succeeding, companies have bought themselves a lot of bad public relations by exercising their legal rights against popular figures. Sony recently courted the disdain of video gamers when they decided to file an application to trademark the term "Let's Play", a common term for videos of people playing videogames.[91] Popular YouTube personalities, The Fine Brothers also suffered a PR backlash when they filed an application to trademark the term "react."[92] The Fine Brothers lost over 170,000 subscribers and eventually abandoned their trademark application.[93]

While these instances both involved trademarks, the underlying principle is clear. Taking legal action against popular institutions is likely to cause a large backlash from consumers. The first website owner to tilt against, let us say, Adblock Plus, will undoubtedly receive some sort of public backlash. Before taking any legal action, it would be wise to consider not only the potential legal outcomes of a lawsuit, but also the potential loss in users that may result.

Ultimately, while a website owner may have a solid legal claim against an AFS company under the circumstances that have been the focus of this piece, website owners and advertisers need to evaluate how to stop users from filtering their content, as well as, why they felt the need to filter their content in the first place.

V. CONCLUSION

The current trends are unsustainable for all parties involved. End users cannot continue to get a free ride and someone needs to pay to keep the lights on. Advertisers and website owners need to reevaluate their advertising strategies. Overly aggressive ads may do more harm than good, and as long as advertisements contain malware, end users have an extremely justifiable reason for using AFS.

Like any other situation, a lawsuit should be a last resort. It is costly, and may alienate valuable users. Hopefully the situation can be resolved in a way that results in a better product for the consumer, and greater profits for content creators.

---

[91] Stephen Kleckner, S*ony Tries to Trademark "Let's Play" and Pisses off the Internet,* VENTURE BEAT (Jan. 8, 2016). http://venturebeat.com/2016/01/08/sony-tries-to-trademark-lets-play-and-pisses-off-the-internet/.

[92] Chris Foxx*, Fine Brothers Spark Fury with YouTube Trademark Attempt*, BBC (Feb. 1, 2016), http://www.bbc.com/news/technology-35459805.

[93] *Id.*