

August 15, 2014

To: Motion Picture Association of America

From: Jenner & Block LLP
Adduci, Mastriani & Schaumberg, LLP

Subject: Use of the ITC to Block Foreign Pirate Websites

**PRIVILEGED & CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION
ATTORNEY WORK PRODUCT
SUBJECT TO COMMON INTEREST AGREEMENT**

This memorandum responds to your request for further consideration of a possible strategy of pursuing an order from the U.S. International Trade Commission (“ITC”) requiring U.S. Internet service providers (“ISPs”) to block traffic from foreign pirate websites. The strategy was first set forth in a memorandum from Jenner & Block to the MPAA dated August 3, 2012 (the “2012 ITC Memo”), and was touched on again briefly in the broader memorandum, dated June 9, 2014 (the “June 9 Memo”), outlining various strategies for obtaining site blocks in the United States. Familiarity with both memoranda is presumed here.

As discussed in the 2012 ITC Memo (a copy of which is attached for convenience), seeking a site-blocking order in the ITC would appear to offer a number of advantages over federal court litigation, at least at first blush. This now seems even more so given the ITC’s recent decision (albeit now on appeal) holding that electronic transmissions are “articles” within the meaning of Section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337.¹ As also discussed in the 2012 ITC Memo, however, such an action would still involve several difficult questions of first impression, making the prospect of success in that forum uncertain. We have given further

¹ See *In the Matter of Certain Digital Models, Digital Data, and Treatment of Plans for Use In Making Incremental Dental Positioning Adjustment Appliances, the Appliances Made Therefrom, and Methods of Making the Same*, Inv. No. 337-TA-833, Comm’n Op. (April 10, 2014) (“Align”). The complainant in the *Align* case appealed the decision to the U.S. Court of Appeals for the Federal Circuit on June 2, 2014, and the respondent appealed the next day. On June 11, the ITC took the unusual step of staying its own cease and desist orders pending the appeal, noting that the case presented an “admittedly difficult question.” Comm’n Op. Granting Stay Pending Appeal at 10 (June 11, 2014). The case is not likely to be decided for at least another year.

consideration to these questions and provide our additional views below, subject to our continued research and analysis.²

In sum, as explained below, we believe that: (1) a site-blocking order against “transit” ISPs – those that carry Internet data across U.S. borders – is not likely to be technologically feasible, and (2) the ITC has the authority, instead, to order network access ISPs to cease and desist from providing their subscribers with access to pirate sites, *but only after* the ITC has found the network access ISPs to have violated Section 337 in connection with either their importation of an infringing work (if we can establish that network access ISPs should be regarded as “importers”) or their distribution of an imported infringing work. It may not be necessary that the ISP’s violation of Section 337 amounts to copyright infringement but could instead be based on either the ISP’s importation of an infringing article, domestic distribution of an imported infringing article, or some other “unfair act,” although the question is not free from doubt. Finally, we also note that, because Section 337 requires an importation of infringing articles, an ITC approach may be especially challenging with respect to torrent sites, where it may be difficult to prove whether the infringing articles (as opposed to the links) emanate from sources inside or outside the United States. That said, the ITC’s willingness to assert jurisdiction over imports of electronic transmissions in the recent *Align* case suggests that the ITC would treat a test case seriously, taking into account all the facts and circumstances without elevating form over substance, notwithstanding several difficult legal questions of first impression.

1. **Is an order requiring “transit” ISPs to block the importation of infringing data from foreign pirate sites technologically feasible?**

As explained in the 2012 ITC Memo, it is important to distinguish between those ISPs that carry Internet traffic across U.S. borders – so-called “transit” ISPs³ – and those that provide Internet access to individual subscribers in the U.S. – so-called “network access” ISPs. As “transit” ISPs are more easily characterized as “importers” of infringing articles given their role in carrying data into the U.S., the 2012 ITC Memo logically focused on those ISPs as potential respondents in an ITC case. *See* 2012 ITC Memo at 18-20.

Having consulted with our technical experts, however, we believe that an order requiring transit ISPs to block traffic from foreign pirate sites raises far more difficult questions of feasibility and efficacy than the site blocks contemplated in either an All Writs Act or Section 512(j) site-blocking order. In particular, an ITC order directed to the transit ISPs would address *inbound* (i.e. “imported”) traffic routed from the foreign site into the U.S., whereas an All Writs

² At your instruction, Jenner & Block has worked closely with the law firm of Adduci, Mastriani & Schaumberg, LLP (“AMS”), who have specialized expertise in ITC proceedings. Although this memorandum reflects the joint input of Jenner & Block and AMS, the two law firms are not affiliated and no such affiliation should be inferred from the fact that this memorandum has been prepared jointly.

³ The 2012 ITC Memo refers to these ISPs as “conduit” or “backbone” ISPs, but they are more commonly known as “transit” ISPs.

Act or Section 512(j) order would address *outbound* traffic from the consumer seeking access to the foreign site, which is how the existing forms of site blocks in Europe are structured. The former is viable (if at all) only on the basis of IP address blocking (because the inbound packets contain no URL or domain name information), whereas the latter allows for more surgical blocking based on URLs within the web requests of users, a method described in Attachment D to the June 9 Memo. As a result, site blocking of *inbound* traffic is technically feasible only with respect to those pirate sites that do not share an IP address with any other site. As previously discussed, a pirate site could easily start to share its IP address with other sites as a countermeasure to an IP-address block, thereby amplifying the problem of over-blocking that IP-address blocking by itself presents.

Moreover, as our technical experts have confirmed, the mere task of defining and identifying the transit ISPs that are responsible for “importation” of data from foreign sites, and which could reasonably be subject to a site-blocking order, is itself daunting. The number of such conduits carrying the majority of traffic between U.S.-based users and a particular foreign pirate site on a given date may be relatively small, but the number that could *potentially* carry such traffic is considerably larger. Because the Internet is designed to route around blocks or choke points, blocking by today’s major transit providers would immediately shift the load to others. And the mix changes in the normal course, regardless of site blocking.⁴ In addition, unlike consumer-facing network access providers, transit ISPs are unlikely to have the equipment necessary to conduct the type of filtering that would be necessary for an effective site-blocking system, as explained in Attachment D to the June 9 Memo. As a result, the imposition of site blocking at these points on the network would likely be regarded as impractical.

2. **Assuming that blocking by “transit” ISPs is not feasible, can consumer-facing network access ISPs be ordered to block their subscribers’ outbound access to foreign pirate sites as a means of giving effect to the remedy against the importation of infringing articles?**

Even though site blocking by transit ISPs may be impractical in most (and likely all) cases, it may still be possible for the ITC to issue orders to the consumer-facing network access ISPs requiring them to cease and desist from providing their subscribers with access to the pirate site. To do so, however, the ITC would first have to find that the network access ISPs, by providing their subscribers with access to the pirate site, have themselves violated Section 337. *See* 19 U.S.C. §1337(f)(1) (authorizing cease and desist orders against “any person violating this

⁴ Most international traffic is carried by a number of submarine fiber-optic cables. However, ownership and control of these cables is not limited to only a few identifiable ISPs that would be subject to blocking orders. Rather, there are multiple layers of separate businesses involved, with physical cable ownership at the bottom and a transit ISP’s logical international network at the top. The number of players grows as one moves up the stack. A graphical representation of the complexity of fiber-optic cable providers can be seen at <http://submarine-cable-map-2014.telegeography.com>. This illustration does not include satellite, microwave/radio or other providers of Internet traffic into the U.S.

section”). Although the question is novel, there is support in ITC practice for such a finding and order against network access ISPs.

A. The ISPs’ Violation of Section 337

Although the scope of what can constitute an “unlawful” act in violation of Section 337 is broad, there are essentially four theories that could most plausibly serve as the basis for a finding of the network access ISPs’ “unlawful” act in these circumstances: (1) that the network access ISPs are engaged in the “importation” of infringing articles, (2) that the ISPs’ domestic distribution of infringing articles constitutes a post-importation “sale” of such articles; (3) that the ISPs’ continued and extensive provision of access to the pirate site is an “unfair act,” as outlined in the 2012 ITC Memo at 15-16, or (4) that the ISPs’ role in the importation of the infringing articles constitutes copyright infringement. *See* 19 U.S.C. §1337(a) (defining “unlawful activities”).

1. Importation. The importation of an article that infringes copyright is an “unlawful” act under Section 337. *See* 19 U.S.C. §1337(a)(1)(B)(1). Because it is the transit ISPs and not the network access ISPs that actually carry the infringing data across the border, we would need to persuade the ITC that the network access ISPs’ conduct is also tantamount to “importation into the United States” of copyright-infringing articles. The term “importation” is undefined in Section 337 and the U.S. Supreme Court, at least historically, has taken a broad and practical approach to determining whether there has been an importation for purposes of U.S. law.⁵ For this reason, we may be able to develop a case that the network access ISPs, by virtue of the integral role that they play in the process of accessing and delivering infringing content from the foreign site to the end user, should be treated as an importer for purposes of Section 337. While network access ISPs are less naturally viewed as “importers” given their purely domestic position on the network, the Federal Circuit may be willing to give the Commission some latitude to define the term broadly to reflect the practical (as opposed to technical) realities of the online marketplace.

2. Sale After Importation. Even if we cannot persuade the ITC that network access ISPs are “importers” of the infringing articles, it can plausibly be argued that the network access ISPs are engaged in a post-importation “sale” of the infringing articles to their end-user subscribers, in violation of Section 337. *See* 19 U.S.C. §1337(a)(1)(B) (providing that “sale after importation into the United States” is an unlawful act). The difficult question presented here is whether an ISP, by providing network access in exchange for its subscribers’ payment, can be found to have engaged in the “sale” of the infringing articles as that term is used in Section 337. *See, e.g., Certain Agricultural Tractors*, Inv. No. 337-TA-380, Notice of Comm’n Determination Concerning Violation of Cease and Desist Orders and Civil Penalty, USITC Pub. No. 3227 (Jul. 28, 1999), 1999 WL 957711 at *26 (“[U]nfair trade practices can be reached by section 337 when such practices involve a ‘sale within the U.S. after importation’ by an importer or an owner.”) (quoting *Certain Hardware Logic Emulation Systems*, Inv. No. 337-TA-383, Comm.

⁵ *Cunard S.S. Co. v. Mellon*, 262 U.S. 100, 121 (1923) (words such as ‘transportation’ and ‘importation’ “are to be taken in their ordinary sense, for it better comports with the object to be attained”).

Op. at 20, 28, 1998 WL 307240 (ITC 1998) (“*Hardware Logic*”). While the ISPs’ commercial service is not easily characterized as a literal “sale” of the infringing articles (as opposed to the sale of general network access and data routing services), we can argue that the term “sale” should be read expansively to include the distribution of articles on the Internet as part of a network access ISP’s commercial service. As the *Align* case demonstrates, the ITC is open to similarly broad constructions of Section 337 to maintain the relevance of the statute to modern modes of online commerce. Under our facts, however, this would be an issue of first impression the resolution of which is difficult to predict.

3. Unfair Acts. Alternatively, we could argue that the network access ISPs, by persistently providing access to infringing foreign sites, have committed an “unfair act” in violation of Section 337. As the 2012 ITC Memo explains, there is a reasonably compelling argument that Section 337 allows for claims based on “unfair acts” distinct from copyright infringement. *See* 2012 ITC Memo at 15-17; *see also* 19 U.S.C. §1337(a)(1)(A)(ii) (defining “unlawful activities” to include “unfair methods of competition and unfair acts in the importation of articles . . . the threat or effect of which is . . . to destroy or substantially injure an industry in the United States”). The range of acts that can be deemed “unfair” under Section 337 is quite broad, and could include a general theory of unfair competition based on such factors as the studios being forced to compete with pirated versions of their own products. While the ITC has decided many unfair act cases, it has not done so in the context where that act is premised on copyrighted works, so this question would be another one of first impression.

4. Copyright Infringement. Finally, as we have discussed, the studios should have a reasonable prospect of proving an ISP’s contributory copyright liability, although such a case would be quite challenging. *See* June 9 Memo at 5-6 and Attachment B thereto. Given the difficulty of such a case as well as the adversity it would create with ISPs more generally, one of the primary goals of the overall site-blocking strategy has been to avoid having to sue an ISP and prove its liability for infringement. We assume, therefore, that the prospect of having to do so in the ITC – a forum with little or no experience with the sorts of complex copyright issues presented here – would not be the preferred approach.

B. The Cease and Desist Order

If we can establish the named network access ISPs’ violation of Section 337, then the ITC would have authority to issue cease and desist orders against those ISPs. Whether that order could include detailed terms requiring the ISPs affirmatively to block their subscribers’ access to the pirate site is another question of first impression – especially when the order would effectively require blocking of *outbound* requests from users rather than *inbound* (*i.e.*, “imported”) traffic from the pirate site. Nevertheless, we believe there is a reasonable basis for the ITC’s authority to do so.

As discussed in the 2012 ITC Memo, the ITC historically has taken a very broad view of its authority under Section 337 to craft remedies directed to unfair trade practices. *See* 2012 ITC Memo at 15, 19-20 (citing authorities); *see also Hardware Logic*, Comm. Op. at 30 (“we have broad discretion to fashion a cease and desist order that provides complete and effective relief for

violations of section 337”); *id.* (“Our remedial authority extends to the prohibition of all acts reasonably related to the importation of infringing products and ... it is not a requirement of section 337 that the unfair trade practice to which the remedial order applies originate outside of the United States”). Because the network access ISPs are the only parties in a position feasibly to implement an effective site block, the ITC could reasonably order the ISPs to do so, based on the ITC’s broad authority to render an effective remedy against the importation of infringing articles. We believe that the Commission would seriously consider such an order, especially in light of the existing track record of site blocking in Europe, as well as the fact that the Copyright Act, in Section 512(j), expressly contemplates site blocking.

3. **Can the ITC order ISPs to block access to pirate link sites that do not host infringing content?**

We also recommend naming the foreign pirate sites as respondents in the ITC investigation. If it can be demonstrated that the foreign pirate sites facilitate the importation of infringing works, even if the importation is actually done from files hosted on other servers, the ITC is very likely to find the pirate sites to be in violation of Section 337 by virtue of their essential role in the transmission (importation) of infringing works into the United States.⁶ The fact that the actual importation is conducted by third parties is highly unlikely to dissuade the Commission from finding a violation by the pirate sites, given relevant precedent. *See* 2012 ITC Memo at 18. While the infringement is more attenuated in such circumstances, we agree with the view that the ITC has the authority to address such “secondary” infringement. *See id.*

It should be noted, however, that our ability to establish a Section 337 violation based on the importation of links alone is uncertain, given that links are not themselves infringing (as opposed to the infringing content files to which they point). For example, in one recent case involving induced infringement of patents, the Federal Circuit held that the ITC lacks authority to find a violation of Section 337 premised on induced infringement through the importation of non-infringing articles that are used to infringe “where the acts of underlying direct infringement occur post-importation.” *Suprema, Inc. v. ITC*, 742 F.3d 1750, 1760 (Fed. Cir. 2013). The *Suprema* decision was recently argued *en banc*, however, so the Federal Circuit’s approach to this issue remains somewhat unclear.

Nevertheless, given the close relationship between link sites and the computers that host and serve the infringing content, the ITC could well be persuaded that the importation of the “file location” information (*i.e.*, the links) – rather than the infringing files themselves – constitutes “unfair methods of competition and unfair acts in the importation of articles” within the meaning

⁶ It is common in ITC cases to name the foreign producer or supplier of the infringing articles as a party, even when third parties are responsible for the actual sale or importation of those articles. Here, the finding of a violation by the foreign pirate sites would be an important part of our case against the ISPs, as it would put the ISPs on notice (through issuance of cease and desist orders) that the importation of the infringing articles from these sites is prohibited. Moreover, placing the focus on the foreign site would help to minimize adversity with the ISPs: even though we are required to show an “unlawful” act on the part of the ISPs, the core of the complaint would be the foreign pirate sites’ acts of infringement rather than the ISPs comparatively “innocent” conduct.

of Section 337, thereby satisfying the importation requirement. Such an approach would be consistent with the ITC's finding in *Align* that the importation of datasets constituted the importation of an infringing "article" even though the imported datasets did not themselves directly infringe the asserted method patent claims in that case but were instead only a step in the patented method (the Commission found that the datasets contributorily infringed). *See also Columbia Pictures, Inc. v. Fung*, 2009 WL 6355911 *9, n.18 (C.D. Cal. 2009) ("Because dot-torrent files *automatically* trigger this content-downloading process, it is clear that dot-torrent files and content files are, for all practical purposes, synonymous") (emphasis in original). While this is a novel issue, the Commission has shown a willingness and ability to grapple with complex legal and factual questions posed by emerging technologies and is likely to give such an argument serious consideration. Still, as noted, the *Align* case is currently on appeal to the Federal Circuit, so further guidance on the Federal Circuit's view of this novel issue will be available only after the Federal Circuit decides both the *Align* and *Suprema* cases.

* * * * *

ADDUCI, MASTRIANI & SCHAUMBERG, LLP
Tom M. Schaumberg
Deanna Tanner Okun
Jonathan J. Engler

JENNER & BLOCK LLP
Kenneth L. Doroshov