The Necessity of Geoblocking in the Age of (Almost) Unavoidable Geolocation (Guest Blog Post)

September 25, 2018 · by Eric Goldman · in Privacy/Security, Trademark

by guest blogger Marketa Trimble

Recent U.S. court decisions suggest that geoblocking might no longer be optional – the use of geoblocking might now be de facto mandatory for any website operator who wants to avoid being subject to the jurisdiction of courts in the United States. This month, another decision concerning geoblocking was handed down, joining the earlier cases I discussed here in May 2017 and March 2018: The U.S. Court of Appeals for the First Circuit’s decision in Plixer Intl. v. Scrutinizer GmbH suggests that courts are growing skeptical of arguments claiming infeasibility or unreliability of geoblocking at a time when many, if not most, website operators want or need to know where their users are located and at a time when geoblocking is becoming cheaper and more reliable.

Plixer is a trademark infringement, unfair competition, and dilution case. Both the plaintiff and the defendant used the mark “Scrutinizer.” The plaintiff has a federal trademark registration for the mark in the United States. The German defendant, while having no U.S. trademark registration, used the mark on the Internet in connection with its own goods and services. At issue was whether the U.S. District Court for the District of Maine, in which the plaintiff brought the case, had specific jurisdiction over the German defendant per Federal Rule of Civil Procedure 4(k)(2), and the only disputed requirement of the Rule was whether the court's exercise of personal jurisdiction comported with due process – meaning whether the German defendant had adequate minimum contacts with the United States.

The German defendant's contacts with the United States stemmed from its Internet presence. It did not specifically target U.S. customers but ran a globally accessible website, was aware that some of its customers were from the United States, and drew income from the United States that the court described as “not insubstantial.” (Id., *6.) It would seem that under these facts the court could have made its conclusion on jurisdiction without addressing the German defendant's failure to geoblock users accessing its website from the United States.

The court did, however, address the defendant’s failure to geoblock. It concluded that while the use of geoblocking is not necessary to limit the territorial scope of activity on the Internet for jurisdictional purposes (a conclusion that was also reached by the U.S. district court in Triple Up Ltd. v. Youku Tudou, Inc.), the use of geoblocking “is surely relevant to [a defendant’s] intent not to serve the United States.” (Id., *5.) Therefore, the court said, the defendant’s “failure to implement such restrictions, coupled with its substantial U.S. business, provides an objective measure of its intent to serve customers in the U.S. market and thereby profit.” (Id., *5.) The court rejected defendant’s argument that geoblocking (which was referred to as “access-blocking technology” in the decision) should be irrelevant because it is an “imperfect, developing technology.” The court called the defendant’s warnings about the state of geoblocking technology “misplaced based on the record before [the court].” (Id., *5.)
A failure to geoblock alone would not have been sufficient for personal jurisdiction in *Plixer*; the facts in the case regarding Scrutinizer’s contacts with the United States would have justified the exercise of personal jurisdiction over the German defendant even without the defendant’s failure to geoblock. Nevertheless, the court chose to address the issue of geoblocking, and the decision is additional evidence that courts are weary of arguments that geoblocking is infeasible, imperfect, or costly, when many or even most Internet actors do check their users’ location and frequently collect and utilize that location information.

The fact that website operators knew of their users’ location was important to courts’ decisions on personal jurisdiction. In *Plixer*, the defendant knew the location of its users; its privacy policy specifically referred to user location as the kind of information that the defendant stored. (Exhibit 4 to the Affidavit by James Goggin, plaintiff’s attorney, docket document 15.) In *Mavrix Photo Inc. v. Brand Technologies, Inc.*, the U.S. Court of Appeals for the Ninth Circuit also took into consideration the defendant’s knowledge of its users’ location – even though the geolocation in the case was used by third-party advertisers who placed their ads on the defendant’s website based on the location of the users. (*Id.*, 10352. For a different result on location-tailored third-party advertising see the unpublished July 17, 2018, appellate decision in *Triple Up Ltd. v. Youku Tudou, Inc.*, where the facts were slightly different from those in *Mavrix*.)

Being oblivious, or choosing to be oblivious, to user location could be more difficult in the future. While collecting location information might have been optional in the past (and used merely for analytical and marketing purposes), the new European Union General Data Protection Regulation makes the determination of user location necessary; if a website operator, regardless of where the operator is located, collects and processes personal data of its users and some of the users are in the European Union, the EU Regulation, which reaches beyond the borders of the EU, requires the operator to comply with its requirements. Given that an operator will know the location of its users, the operator should consider how its decision not to geoblock, should it choose not to do so, might be viewed by the courts when they consider the reach of their adjudicatory jurisdiction.
Ralph Haygood • 8 days ago

Yesterday, I tried to post a comment, but for reasons unfathomable, Disqus decided it was spam. I'll try again and keep it short.

Please explain how this decision is enforceable against a company with no physical presence in the USA. As someone with no experience of such things, I find this puzzling.

Eric Goldman • 8 days ago

I don't know why Disqus chomped it. Here is the full comment: "I am not a lawyer. Please explain to me how, exactly, this ruling is enforceable against a company with no physical presence (and barely any other kind of presence) in the USA. Is it assumed that a German court will be willing to enforce it? (What I've read about such things indicates that getting a foreign court to enforce a judgment from an American court tends to be difficult.) Will they order every ISP in the USA to block Scrutinizer? Will they order every credit card issuer in the USA to reject purchases from Scrutinizer? Or what? Forgive me if my questions are naive, but this ruling strikes me as Alice-in-Wonderland-ish.

To the extent it isn't Alice-in-Wonderland-ish, it's more than disturbing. Consider the obvious implications. For example, consider a software company incorporated in New Zealand, which has practically abolished software patents, but that has at least one customer in the USA, which is infested with patent trolls. By the logic of this ruling, said company is vulnerable to attack by said trolls. Even if, when attacked, the company blocks all traffic it suspects of being from the USA, (1) a troll might try to get a judgment pursuant to the period when traffic from the USA wasn't blocked, and (2) whatever the judges of the First Circuit may imagine, geolocation is far from perfect, so some traffic from the USA may well leak through, and if a troll can demonstrate as much, it can try to get a judgment pursuant to this continuing "violation". Even if the claims of the trolls were without merit, as they usually are, the possibility of having to settle such attacks, at a cost of quite possibly tens of thousands of dollars each, or to fend them off, at a cost of quite possibly hundreds of thousands of dollars each, is so
threatening that it would seem the company has little choice but to block all traffic it suspects of being from the USA starting the day it launches, to post prominent notices stating that it will not knowingly do business with Americans, and, even after all that, to hope for the best.

Now multiply that by 193, the number of countries in the United Nations, or so. This kind of thing has the potential to place web site operators under a genuinely crushing burden. If I'm potentially liable for breaking the laws of every country on Earth merely because some of their citizens access my web site, then I'm living on borrowed time unless, like Facebook or Google, I can afford to spend millions of dollars defending myself whenever and wherever I'm attacked. This is madness."

Ralph, your points are very good; thank you for your comments.

On enforceability, it depends on whether the defendant has any assets in the United States. But of course many defendants will simply abide by the U.S. court decision because they plan to do more business in the United States in the future and don’t want to face the potential negative consequences of noncompliance.

The chilling effects are not to be underestimated. Many foreign defendants might give up fighting a case as soon as a decision on jurisdiction comes down and simply stop offering their goods and services in the United States in order to avoid incurring any additional litigation costs.

Note that the courts have not said that website operators must use geoblocking to avoid personal jurisdiction in the United States. The lack of geoblocking was only one of several facts that the courts have considered. At least for the purposes of determining whether the courts have personal jurisdiction over a defendant, it was not important whether geoblocking would be perfect, effective, or good, but it was important that the defendant did not even try to implement geoblocking even as the defendant was determining where its users were connecting from. So geoblocking is not necessary if a website operator takes other measures, such as having a disclaimer on its website and/or not offering goods and services to customers in the United States.

Thanks.

Thanks.