

The PROTECT IP Act – Warning: This Bill May Cause Seizures

If a lawmaker were to mix the overzealous propaganda of the USA Patriot Act with the overreaching executive authority of COICA, the new PROTECT IP Act would probably be the result. This new version of COICA, chock full o' censorship issues, but with a shiny new name was recently introduced to Congress. Say hello to the [“Preventing Real Online Threats to Economic Creativity & Theft of Intellectual Property” \(PROTECT IP\) Act.](#)

Had it not stalled after its committee approval last year, [COICA](#) would have allowed federal authorities to seize domain names of sites using infringing content and require ISPs to cut off user access to the rogue sites. Well, the PROTECT IP Act raises the stakes a bit. The Act seeks to set up a system whereby the government, or private parties, can file suit against domain names that are tied to websites allegedly dedicated to infringing activity, get a preliminary court order based on one-sided evidence, and use that court order to force third party service providers like hosts, registrars, payment processors and others, to effectively shut down the site.

This means that any entity providing services to an allegedly infringing site can be dragged into the suit; even “internet location tools.” That’s right, search engines. Under the proposed legislation, these third parties have every incentive to do the government’s bidding, and even police their customers’ activities, since the Act provides an immunity from claims resulting from actions taken by a service provider against a site where the provider has a “good faith belief” that the site is “dedicated to infringing activities.” Host and billing companies beware; ‘you’re either with us or you’re against us’ in this Bill.

Just like they did last year with COICA, supporters of the Act cite to its “safeguards” in defense of the anticipated backlash. These purported safeguards include the ability of an affected site to “petition the court to suspend or vacate the order” in question. As you might guess, the “safeguards” are implemented *after* the feds get the ball rolling and the involved service providers have already been forced to discontinue services or access to the site. In other words, censor first, ask questions later...

Equally disturbing is the Act’s “private right of action” provided to IP owners. Rights holders, along with the government, will have the ability to pursue legal action against websites that are allegedly infringing on their IP rights and other affiliated third party intermediaries such as a payment processor or “online advertising network.” The import of this provision cannot be understated. The obligations imposed on service providers could change dramatically if they face being dragged into private lawsuits based on their customers’ activities. As the [Electronic Frontier Foundation](#) accurately pointed out, “Consider whether Viacom would have bothered to bring a copyright infringement action against YouTube—with the attendant challenges of arguing around the DMCA safe harbors—had it had this cause of action in its arsenal. The act includes language that says it's not intended to ‘enlarge or diminish’ the DMCA's safe harbor limitations on liability, but make no mistake: rights holders will argue that safe harbor qualification is simply immaterial if a site is deemed to be dedicated to infringement.”

The one benefit offered by the PROTECT IP Act is a new, narrower definition of proscribed websites characterized with the infamous phrase of “dedicated to infringing activities.” The previous definition used in COICA was overly vague to the extent that it would have likely put legitimate websites at risk of

violation. That definition, although admittedly much more lenient than its predecessor, is only a slight concession in the grand scheme of things.

Of greatest concern, from a First Amendment perspective, is the increased likelihood of pretrial seizure of domain names that are alleged to be in violation of the Act. Registrars, or even registries, are likely included in the category of service providers subject to the new Bill. Shutting down an entire venue of communication based on a preliminary finding that it is dedicated to infringing activities, before a trial or other judicial determination on the merits, runs counter to all Free Speech principles. That's why the government cannot shut down a bookstore just because a clerk gets arrested for selling an allegedly obscene book. However, the concept of the government seizing domain names, the same domains that are home to constitutionally protected speech, and that seizure occurring before any defenses are heard, reeks suspiciously of what we constitutional lawyers call "prior restraint." That, simply, is not allowed.

This disturbing trend of seizing domain names made headlines just a few weeks ago in what has come to be known in online gaming circles as "[Black Friday](#)." On April 15, 2011, the United States DOJ issued an [indictment](#), and filed a [civil suit](#) against the three largest online poker sites in the world; Poker Stars, Full Tilt Poker and Absolute Poker. As a result, the .com [domain names for each of the sites were seized](#) for ultimate forfeiture to the government, as alleged instrumentalities of the "crime." What crime? Well, since Internet poker is technically not against any federal law, the DOJ dug up some New York misdemeanor statutes which generally prohibit gambling and related promotional activities as the purported basis for the gambling charges, and the multimillion dollar seizures of domain names and bank accounts. But the applicability of this state statute to licensed foreign gaming activities is questionable at best. Regrettably, however, due to some accompanying bank fraud charges, it is unclear whether or not this case will determine once and for all if online poker is illegal. Regardless of the ultimate outcome, the DOJ has made clear that it will seize any domain name – at the registry level – that it deems to be used in the violation of U.S. law – even if operated from overseas, in full compliance with the host country's laws.

Granted, the online gaming industry is no stranger to cyber seizures; [Kentucky v. 141 Internet Domain Names](#) has been making its way through the court system for almost three years. In this [case](#), the state of Kentucky demanded that various registrars surrender domain names of sites acting as "gambling devices." There, the state obtained a pretrial seizure order for the domain names, and emailed the order to the sites' registrars. Some of the domestic registrars complied, but most of the foreign registrars ignored the court order, as coming from an improper jurisdiction. The key distinction between the *Kentucky* case, and the recent federal online poker domain seizures, is the level at which the domains were seized. On Black Friday the feds double jumped over the registrars, which were all outside the U.S., and went right to the .com registry to enforce its pretrial seizure order. And since all .com domain names are controlled by a U.S.-based registry, there was no jurisdictional issue to worry about.

A few domains have already been seized, under existing intellectual property laws. In November of 2010, the feds [seized](#) a number of domain names on grounds of copyright infringement and

counterfeiting. As this post goes to publication, it appears that the DOJ has seized another handful of [online gambling domains](#). The government even created its own [undercover payment processor](#) to get the sites to sign up. So the trend shows no sign of letting up.

There is no denying the detrimental impact that piracy is having on the adult industry. Copyright infringement should be punished, consistent with due process principles. But the idea of allowing the government to shut down websites by seizing their .com domain names, based on one-sided hearings and allegations of infringement or counterfeiting – without consideration of the merits or defenses, sets a dangerous constitutional precedent. Simply substitute “obscene” for “infringing” and you get the picture.

*Lawrence G. Walters, Esq., heads up [Walters Law Group](#), a law firm which represents clients involved in all facets of the adult industry. The firm handles First Amendment cases nationwide, and has been involved in Free Speech litigation at all levels, including the United States Supreme Court. All statements made in the above article are intended for general informational purposes only and should not be considered legal advice. Please consult your own attorney on specific legal matters. You can reach Lawrence Walters at larry@firstamendment.com. More information about **Walters Law Group** can be found at www.FirstAmendment.com.*