



November 15, 2010

The Honorable Patrick Leahy
Chairman
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510-6275

Re: S. 3804, The Combating Online Infringement and Counterfeits Act (COICA).

Dear Chairman Leahy:

NetCoalition¹ has serious concerns with S. 3804, the Combating Online Infringement and Counterfeits Act (COICA), which is on the agenda for the Committee's November 18 executive business meeting. COICA is intended to address the problem of foreign websites that are otherwise beyond the reach of U.S. legal process that make infringing content available to U.S. users. We understand your frustration that the many actions taken by the Committee to address online infringement, including the PRO-IP Act adopted in the 110th Congress, appear not to have caused a meaningful reduction in the level of infringement. We support your objective of combating counterfeiting and online infringement. Nonetheless, the bill raises significant legal, political, and technical issues that need to be considered and resolved before it progresses. Accordingly, the legislation should not be reported out in the lame-duck session. Instead, it should proceed by regular order in the 112th Congress.

COICA authorizes the Justice Department to bring *in rem* actions against domain names of websites dedicated to infringing activities. If the domain name has a foreign registry, the Justice Department can serve the order issued against the domain name on the operators of domain name system servers, financial transaction providers, and advertising networks, which would then be required to discontinue providing services to these websites. This new *in rem* proceeding raises a host of questions that necessitate thorough review.

1. Interaction with U.S. Legal Process. It is our understanding that COICA is intended as an extraordinary remedy where a foreign, rogue website is otherwise not reachable by U.S. legal process. Where a website (whether foreign or domestic) is willing to appear and defend in U.S. courts, existing legal rules should be applied and COICA should not supplant or supercede those proceedings. This is the approach, for example, that Section 512(g)(3) of the Digital Millennium Copyright Act (DMCA) employs with respect to allegedly infringing content hosted on behalf of foreign users. The current draft does not ensure that COICA will not be used as a weapon against the domain names of

¹ NetCoalition serves as a public policy voice to leading Internet and technology companies, including Amazon.com, Bloomberg LP, eBay, Google, IAC, Yahoo!, and Wikipedia.

sites that are not "rogues," but are instead willing to defend their actions in U.S. courts.

2. Jurisdiction. COICA would authorize a U.S. court to exercise jurisdiction over a foreign-registered domain name by virtue of the impact the foreign website associated with that name may have on U.S. rightsholders. It is far from clear that the due process clause of the U.S. Constitution allows a U.S. court to exercise jurisdiction in this manner.

Moreover, this approach could set a dangerous precedent for foreign countries to attempt to control content on U.S. websites. As you may recall, a French court found Yahoo liable for hosting auctions of Nazi paraphernalia that were viewable in France. Similarly, an Australian court exercised jurisdiction over Barron's for alleged defamation in an article posted on a U.S. website. The issue of jurisdiction for Internet-based activity is extraordinarily complex. Until now, Congress has let the courts take the lead on how to apply traditional principles of jurisdiction to the Internet environment. The Committee must carefully consider the implications of this aggressive assertion of jurisdiction on U.S. websites that are viewable overseas.

3. Extraterritoriality. In addition to authorizing U.S. courts to exercise jurisdiction over foreign activity, COICA creates extraterritorial remedies. A financial transaction provider would be required to prevent the use of its trademarks on foreign websites. Similarly, an advertising network would be required to stop placing contextual or display ads on foreign websites. This would be the case even if a U.S. user no longer can access the site or purchase infringing material from it. Once again, this could be a dangerous precedent that could be exploited by other countries against U.S. businesses.

4. Due Process. Under COICA, once a court issues an injunction against the domain name of a website dedicated to infringing activity, the Justice Department can serve the order on the operators of domain name system servers, financial transaction providers, and advertising networks. These entities would then be required to discontinue providing services to these websites. COICA, therefore, allows the Justice Department to impose obligations on these entities without first giving them an opportunity to be heard in court. In other words, the operators of websites dedicated to infringing activity receive more procedural protections than these innocent service providers.

4. Secondary Liability. The new *in rem* proceeding could also have an unintended impact on copyright and trademark secondary liability. Since secondary liability in these areas is entirely judge-made, it is constantly evolving, and the language of COICA could easily shift the careful balance struck by existing law. For example, the standards in the definition of sites that are "dedicated to infringing activities" differ from those in recent judicial decisions relating to secondary copyright and trademark infringement. The new *in rem* proceeding could affect this precedent. Similarly, as noted above, COICA requires the operators of DNS servers, financial transaction providers, and

advertising networks to take certain actions when served with orders issued under this statute. Courts could infer from this provision a Congressional intent that secondary liability be extended to such entities. Although COICA contains a savings clause, it may not be strong enough to prevent these effects on secondary liability.

Furthermore, potential interaction between COICA, secondary liability, and the DMCA safe harbors could unintentionally expand the scope of the legislation, reaching a much broader array of intermediaries than those identified in the bill. For example, once a site is identified as "dedicated to infringing activity," would that constitute "red flag knowledge" sufficient to strip online service providers who provide hosting or search engines of their DMCA safe harbor protections? If so, what would their legal obligations be with respect to such sites? Moreover, because the DMCA safe harbors are limitations on liability, rather than affirmative defenses, under the existing language of COICA sites that fully qualify for the DMCA safe harbors could nevertheless find themselves declared to be "dedicated to infringing activity" because they technically "violate" Title 17 despite enjoying a limitation on resulting liability. These subtle interactions are not fully addressed by the proposed savings clause.

5. Internet Stability. COICA could also undermine the stability of the Internet. By requiring DNS server operators to block domain names, COICA encourages users to take the easy step of switching from their ISP's name servers to offshore name servers. This, in turn, diminishes the ability of the U.S. government and ISPs to respond to cyber-attacks. According to computer security expert Dan Kaminsky, "the best place to deploy DNS filters is at the users' ISP name server. But these filters will become useless once users abandon their ISP name servers."² The shift away from ISP name servers also diminishes the ability of network managers to monitor the overall activity of the network. ISP name servers "provide an extraordinarily valuable, even predictive, data stream regarding malicious behavior. Losing this stream would materially degrade our ability to secure cyber space." Additionally, a migration away from ISP name servers will make it more difficult to distribute software patches to users. "Now, with DNS [Security Extensions] finally offering the real fix for cache poisoning, we see a proposal that will cause users to avoid the very servers we've spent a decade trying to secure and to get people to use."

Significantly, because of the ease of selecting an offshore name server not bound by COICA, COICA will deter few users' intent on accessing infringing content. Thus, COICA would render the Internet more vulnerable to cyber-attacks, but have little impact on infringement.

6. Voluntary Actions. The draft manager's amendment provides a safe harbor from liability for a domain name registrar that voluntarily blocks domain names of

² Dan Kaminsky, DNS Filtering and S. 3804, "Countering Online Infringement and Counterfeiting Act," Oct. 2010.

websites it “reasonably believes” are dedicated to infringing activity. This provision can be abused for anticompetitive purposes. Many domain name registrars provide other services, and they may take advantage of the safe harbor to block access to a competitor’s website. Given the breadth of the definition of a website “dedicated to infringing activity” (see below), it would be easy for the domain name registrar to have a reasonable belief that a competitor’s website that allows users to upload content is dedicated to infringing activity.

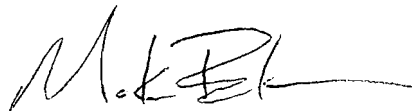
Furthermore, this provision may have implications for secondary liability. A domain name registrar, financial transaction provider, or advertising network could be sued by a rightsholder under a secondary liability theory for failing to take actions that would have been protected by the safe harbor.

7. Definitions. COICA contains undefined or broadly defined terms. Of gravest concern is the sweeping definition of a website “dedicated to infringing activity.” A parsing of the definition reveals that any website used for the distribution of copies with a retail value of \$1,000 could be considered a website dedicated to infringing activity. Thus, any popular website that allows users to upload content would be subject to COICA’s remedies.

Because of the complex and controversial issues COICA raises, it should not be considered during the lame-duck session. Instead, in the 112th Congress the Committee should hold a series of stakeholder discussions on the nature of the problem the bill seeks to address, the constitutionality of the *in rem* procedure, the foreign policy implications of this approach, the impact of DNS blocking on Internet stability, and means of mitigating unintended consequences on innocent service providers. After the stakeholder discussions, the legislation should proceed in regular order.

We look forward to working with you and your staff on this issue in the 112th Congress.

Sincerely,



Markham C. Erickson
Partner, Holch & Erickson LLP and
Executive Director, NetCoalition

Cc: Senate Judiciary Committee