Thomas M. Dailey
Vice President and Deputy General Counsel
Verizon Communications Inc.

Testimony before the Senate Committee on the Judiciary

Chairman Patrick Leahy (D-VT)

February 16, 2011

I. Introduction

Chairman Leahy, Ranking Member Grassley, members of the Senate Judiciary Committee, thank you for the opportunity to testify today and to present Verizon's perspectives on the Combating Online Infringement and Counterfeits Act ("COICA"). Verizon supports the efforts of Congress, the Department of Justice ("DoJ") and rights-holders to combat the theft of intellectual property carried out through the unlawful sale of goods and copyrighted works on websites. We believe that responsible members of the Internet ecosystem should work with Congress, law enforcement and the courts to take efficient, effective and judicially-sanctioned steps to address this important problem. However, we also note that one of the greatest strengths of the Internet is its ability to promote the open and free-flow of information, ideas and commerce. While Verizon supports the use of strong actions against online actors who egregiously flaunt U.S. law from abroad, we also have always stood solidly on the side of the free flow of information on the Internet – domestically and internationally.

As a major provider of the global internet, we respect and protect the rights of users to pursue their individual and collective desire to connect, create and collaborate. That is why the use of new approaches like those in COICA requires careful

consideration in the broader context of our nation's larger global interests in the growth and health of the Internet, including the promotion of U.S. commercial interests. Verizon believes that the further changes described below are necessary and will help to address these important interests and ensure that the mechanisms described in the bill remain efficiently and effectively focused, but we also urge the Committee to consult further with a broader base of stakeholders about its policy impacts before Congress acts.

II. Discussion

A. The Legislation Should Minimize the Impact on Service Providers.

Because COICA shifts the burden of protecting the property interests of others to network operators, these newly imposed obligations should be limited in nature and scope. Accordingly, Verizon appreciates the fact that the Committee has included in the legislation a number of provisions designed to minimize the bill's impact on Internet service providers ("ISPs"). For example, the limitation that ISPs will be required to take action only pursuant to a judicial order in a lawsuit filed by the Department of Justice will help ensure that ISP resources are not drained by myriad private investigative efforts and that COICA is properly and narrowly invoked.

Similarly, the legislation properly limits the steps a service provider is required to take to prevent a domain name from resolving to that domain name's Internet protocol ("IP") address. For instance, a service provider is not required to modify its networks or take any steps with respect to domain name lookups not performed by its own domain name servers. Finally, because an ISP is acting pursuant to court order, the legislation takes appropriate steps to protect the service provider from liability. The legislation

clarifies that nothing under COICA affects a service provider's limitations on liability under Section 512 of the DMCA, and includes appropriate immunities for taking action in compliance with the legislation or arising from a judicial order issued under it, and protections against liability based on actions taken by subscribers to circumvent DNS restrictions or a service provider's good faith inability to restrict access to a domain name subject to judicial order.

B. Portions of the Legislation Which Verizon Believes Require Amendment or Clarification.

The overbroad or inappropriate exercise of the powerful tools that would be created by COICA would not only place undue burdens on service providers, but would also run counter to U.S. interests in other areas of national import, including promotion of a "global" Internet — an Internet that is not split up by specific national interests or regimes. To limit these dangers while facilitating action against egregious online actors, Verizon believes a limited number of further changes are required to ensure that COICA becomes and remains a narrowly tailored tool that is able to be used, as this Committee's December 17, 2010 report (the "Senate Report") envisions, to help prevent inadvertent access to the "worst of the worst" Internet sites.

First, the bill must be clarified to ensure that service providers are required to take action only with respect to their U.S.-based DNS servers. Second, the legislation should expressly forbid private rights of action and require that DNS restrictions are imposed only where they are the least burdensome form of remedy. Third, from an operational perspective, COICA should be modified to ensure that i) actions against nondomestic domain names are properly and narrowly tailored; ii) the list of restricted domain names is properly administered and service providers receive timely notification from the DoJ of

domain names that no longer require restriction; and iii) appropriate limits are placed on the number of domain names that can be subject to restriction and that cost recovery be made available to service providers which request it. We address each of these issues in turn, below.

1. Judicial Orders to Restrict Access to Domain Names Should be Limited to U.S.-Based DNS Servers.

The bill should clarify that judicial orders issued pursuant to it apply only to service providers' DNS servers located in the United States. While Verizon believes that the scope of the bill's domain name restrictions is intended to apply only to a service provider's U.S. customers and operations, some service providers – including Verizon – maintain DNS servers that are located in countries outside our borders that serve customers outside the U.S. For example, Verizon's overseas affiliates maintain DNS servers abroad that are available to Verizon's non-U.S. based enterprise customers. A judicial order directing a service provider to restrict access to domain names on its international servers – and therefore to international Internet users – not only increases the burden on and cost for service providers, it may create an extra-territorial impact that could open the legislation to legal challenge in foreign courts against which the bill does not and can not provide immunity.

Clarifying the legislation in this way would not materially undermine the bill's goals. For technical and other reasons, we believe most U.S. broadband customers utilize DNS servers designated by their service provider, and we further believe that most U.S. service providers utilize U.S.-based DNS servers for their U.S. customers. Thus, a judicial order restricting access to domain names through U.S.-based DNS servers only

would still carry out the bill's sole objective of limiting inadvertent access to illegal websites by consumers in the United States.

Accordingly, to accomplish the clarification that a judicial order shall only apply to a service provider's U.S.-sited DNS servers, we urge the Committee to make the following highlighted change to §2(e)(2)(B)(i)(I)(bb):

> "(I) such entity shall not be required — . . . (bb) to take any steps with respect to domain name lookups not performed by its own domain name system server ***or domain name system servers located outside the United States."***

2. <u>The Bill Should Expressly Prohibit Private Rights of Action and Ensure that Domain Name Restrictions are Imposed Only Where they are the Least Burdensome Form of Remedy</u>.

Verizon strongly believes that only the DoJ should be authorized to bring an action under the bill and that the law should expressly state that no private right of action is available. The legislation represents a new approach to dealing with the harmful effects of online infringement. Legally mandated restrictions on access to information available through particular domain names, and the resulting creation of a unique, U.S.-specific DNS capability, is something that should be approached with caution and control, with the added protection that only DoJ review brings.

The DoJ is in the best position to offer an unbiased and disciplined review of requests for enforcement under this bill, requests that are intended to restrict access to information on the Internet and which will inevitably create divergence between U.S.-distributed and globally-available DNS information. Having the DoJ serve this important oversight role will help insure that cases brought are properly and narrowly tailored to effectuate the expressed purpose of the legislation of targeting, as the Senate Report

notes, the "worst of the worst" Internet sites. Conversely, private plaintiffs, unlike the DoJ, are acting in their own interests and are far less likely to weigh the costs that their enforcement requests impose on third parties and, more broadly, U.S. national interests in promoting a global Internet. Allowing private litigants to seek judicial orders restricting access to publicly-available websites elevates the risk of over-broad implementation of domain name restrictions.

This concern is not hypothetical. Private parties seeking the identity of Internet subscribers have, at times, swamped the capability of certain ISPs to respond to lawful requests. Recently, for example, plaintiffs in a somewhat different but related context subpoenaed the identities of nearly *ten thousand* Internet subscribers from multiple ISPs, seeking to identify the names of alleged peer-to-peer infringers of certain movie titles. This mass copyright suit swamped the capacity of certain third party ISPs who were subpoenaed to respond, and required those ISPs in some cases to seek protective orders to deal with the extraordinary numbers of IP lookups they were asked to perform.

We also urge the Committee to include a proviso that no relief may be ordered against a service provider unless the relief is the least burdensome among comparably effective forms of relief for that purpose. For example, if content available through a foreign-registered domain name is actually hosted on servers located in the U.S., DoJ should be required to pursue shutdown of that U.S.-based website before seeking a domain name block under COICA against the foreign-registered domain name associated with it. Such language can help ensure that the relief is carefully tailored to achieve the intended purpose.

Accordingly, we propose the following amendment to Section 2(i) to address private right of action point (new language is in ***bold italics***):

> "i) ***NO PRIVATE RIGHT OF ACTION;*** SAVINGS CLAUSE —
>
> (1) IN GENERAL.—Nothing in this section shall be construed to ***create any private right of action, nor to*** limit or expand ***any*** civil or criminal remedies available to any person (including the United States) for infringing activities on the Internet pursuant to any other Federal or State law."

In addition, we propose that the following subsection be added to Section 2(e)(2)(B)(i) to address the "least burdensome" approach point:

> "(III) no relief may be ordered against a service provider unless it is the least burdensome among comparably effective forms of relief for that purpose;"

3. Proper Implementation of the List of Nondomestic Domain Names and Proper Notification to Service Providers of Domain Names No Longer Subject to Restriction are Critically Important.

Implementing a workable mechanism to enable DNS server restrictions on a dynamic list of domain names across potentially dozens or hundreds of U.S. service providers will require considerable coordination and collaboration, and clearly documented processes. Accordingly, Verizon urges the Committee to amend the legislation to instruct the Attorney General to work with service providers to develop administrative procedures and controls in several areas.

First, procedures need to be developed that will insure actions taken against nondomestic domain names are limited to just the domain names that are currently the subject of a judicial order. Such procedures are necessary to reduce the risk of over-blocking and to minimize the administrative burdens associated with ongoing implementation of a dynamic list of domain names.

Second, procedures need to be developed that will insure all U.S. service providers are given prompt notice of a court order to restrict access to a domain name(s). Such procedures are necessary to ensure that domain name restrictions are implemented consistently across all service providers in the U.S. The compliance burden should not fall on just a few service providers, nor should U.S. customers of one service provider have their DNS queries returned unresolved while U.S. customers of another service provider do not. A significant amount of logistical effort will be required to ensure uniformity and transparency in the implementation of this program across all U.S. service providers.

Third, the legislation should instruct the Attorney General to work with service providers to implement efficient mechanisms by which the DoJ will post, maintain and update the list of domain names where access needs to be restricted, and notify service providers promptly when a domain name needs to be removed from the list. Service providers should not be left to try to assemble, track and maintain lists of domains to be restricted over time. Ideally, there will be a single point of reference, maintained by DoJ, that will contain a list of domain names that are subject to judicial orders, and this single point of reference would be affirmatively updated by DoJ, with notice to service providers when domain names have been added to or removed from the list of restricted domains.

These administrative procedures and safeguards are important for several reasons. First, clear rules of the road make sense as a matter of administrative efficiency for DoJ and the service providers affected. Second, network performance issues can potentially result from restricting large numbers of domain names in service provider DNS servers,

so the domain names subjected to a judicial order need to be properly and narrowly tailored and the list of restricted domain names needs to be properly maintained. Third, if a domain name no longer needs to be restricted, it should properly and expeditiously be removed from the list to avoid imposing the restriction longer than legally necessary.

The current version of the bill is silent on these important administrative controls and procedures, but it does provide a vehicle in Section 3 to clarify that DoJ should be tasked with implementing them. Verizon strongly recommends that the legislation be amended to address these administrative concerns by adding the following subsection to Section 3 of the bill:

> "The Attorney General shall –
>
> (7) develop, in consultation with service providers, procedures by which the Attorney General will – identify the specific nondomestic domain names to be the subject of a judicial order under this section; notify all service providers of the domain names which will be subject to such judicial order; maintain and timely update the list of such domain names; and promptly notify service providers when a domain name needs to be removed from such list."

4. The Bill Should Limit the Number of Domain Names to which Access can be Restricted and Provide for Cost Recovery.

The legislation should limit the volume of requests service providers are required to implement and instruct the Attorney General to provide a mechanism for cost recovery. As currently envisioned, this bill is just one tool, intended to be used to address only inadvertent access to the "worst of the worst" Internet web sites. As a practical matter, however, given the tens of millions of domain names in existence, and the virtually limitless number of possible domain names across the .com, .net, and hundreds of country-specific and new top-level domain names, it is reasonable to assume that the

volume of domain names to be blocked under COICA will quickly increase. As the restricted domain names list lengthens, depending on a service provider's infrastructure, one might expect to see performance degradation and delay in the process of DNS queries not just for the restricted domain names, but for all queries to such servers**.** This type of impact might hit disproportionately on small and rural broadband providers who may not have the means to invest in the latest and best server technology.

Therefore, in order to ensure that the list of domains to be restricted under COICA remains a list of the then-current, worst examples of websites engaged in illegal activities, there needs to be a hard limit set on the number of domain names that service providers are required to administer. Such a limit will serve as a natural check on an overly-expansive use of COICA.

In addition, Verizon believes some form of cost recovery is required for the time taken to implement changes in service provider DNS systems. Service providers may need to hire new personnel and make equipment upgrades in order to respond expeditiously to the volume of orders, and will need to take time to re-configure their DNS servers every time they receive a blocking order. Requiring compensation to service providers for the time required to comply with COICA — like hard caps on the numbers of domains to be blocked — will help serve as a natural check on the expansion of the use of COICA.

Such cost recovery mechanisms are not new and have been built into other laws where network providers are required by law to comply with law enforcement requests for assistance. For example, the Electronic Communications Privacy Act ("ECPA") contains provisions for the reimbursement of costs to communications providers for

assistance in accomplishing an interception or in providing certain information that is subject to a lawful request. We believe similar cost reimbursement – tied to the volume of domain names for which access is restricted – is appropriate to offset service provider costs of complying with judicial orders under COICA.

Accordingly, Verizon proposes addition of the following subsection to Section 2(e)(2)(B)(i) to address the domain name cap and cost recovery issues:

> "(IV) no service provider may be required to prevent access under this section to more than 100 domain names at one time, unless the Attorney General arranges for a mechanism through which rights owners who submit information to initiate an investigation under this section furnish the government with funds sufficient to reimburse the service provider for its actual, non *de minimis* costs associated with blocking more than 100 domain names at one time; provided that, for service providers with fewer than 100,000 users the foregoing thresholds shall be set at 50 domain names;"

Thank you for this opportunity to present Verizon's perspectives regarding this legislation.