ITIF
The Information Technology & Innovation Foundation

PIPA/SOPA: Responding to Critics and Finding a Path Forward

BY DANIEL CASTRO | DECEMBER 2011

All stakeholders in the Internet ecosystem should come together to find fair solutions that both protect the rights of IP rights holders and respect the unique challenges of the Internet economy.

The problem of online piracy continues to grow in the absence of stronger government action. Today almost one in four bits on the Internet is attributable to copyright infringing content, despite existing efforts by the content industry and others to limit piracy.[1] In addition, the nature of online piracy continues to evolve in response to changes in technology. Online piracy is no longer limited to college students trading files in their dorm rooms; it has grown into a multi-million dollar international business and widely affects the producers of movies, music, software, books, video games and other forms of digital content. Russian businesses like Legalsounds.com and MusicMP3.ru offer consumers around the world illegitimate access to music through a seemingly legal website. Moreover, a recent study found that profit-driven entities were responsible for publishing 30 percent of the (mostly infringing) content on BitTorrent (accounting for 40 percent of downloads).[2] And while some claim that piracy hurts only the content industry (as if this is not important), it is important to realize that piracy reduces jobs, exports, and overall U.S. competitiveness and standard of living.

Intellectual property (IP) infringement on the Internet is not limited to digital content. Counterfeit goods, often of poor quality, are widely available online through retail websites

and online auctions. Counterfeiters sell goods such as infant formula or baby shampoo that expose young children to serious health risks. Illegal online pharmacies sell counterfeit prescription and non-prescription drugs to consumers for a variety of health conditions. At best, these drugs may simply be ineffective; at worst, they can be harmful, or even lethal, to consumers. Consumers shopping online may inadvertently purchase counterfeit goods, especially luxury goods such as jewelry, cosmetics, handbags, garments and shoes. Often these products are sold on sites that appear legitimate, charge reasonable prices, and may even link to the customer service of the brand owner. A 2011 study found that traffic to forty-eight sites selling counterfeit goods averaged more than 240,000 visits per day or more than 87 million visits per year.[3] As Director of Immigration and Customs Enforcement John Morton put it, "Intellectual property violations have become big-time international crime. We've got to focus and do something about it."[4]

Against this backdrop, in September 2010, Senators Patrick Leahy (D-Vermont) and Orrin Hatch (R-Utah) introduced S. 3804, the Combating Online Infringement and Counterfeits Act (COICA), one of the first serious efforts by Congress in recent years to crack down on online piracy and counterfeiting.[5] A modified version of COICA was introduced in 2011 in S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act or PIPA). Most recently, Rep. Lamar Smith (R-Texas) and his co-sponsors introduced H.R. 3261, the Stop Online Piracy Act (SOPA). While these bills have important differences, many of their enforcement mechanisms are the same. In particular, the legislation enables Internet intermediaries, including Internet service providers (ISPs), payment processors (e.g. credit card companies), ad networks, search engines, domain registrars, and domain registries to take action against websites that are dedicated to infringing activities, in particular foreign sites that are otherwise outside of the jurisdiction of U.S. law enforcement and current remedies.

PIPA/SOPA has generated considerable controversy, much of it driven by false or misleading information. Much of this has been driven by "Internet exceptionalists." For these advocates, the Internet is inherently different from the offline world and should be off-limits to the societal rules that a democratically-elected government wants to impose on it. Any attempt to impose limitations on illegal activities is decried as the first step to totalitarian repression. For example, the Electronic Frontier Foundation (EFF), using some especially over-the-top language, calls SOPA "censorship," a "massive piece of job-killing Internet regulation," and claims it will "break the Internet."[6] As we will show in this report, these claims are completely false.

Some criticism of PIPA/SOPA is driven by individuals and interests groups who oppose the current state of U.S. copyright law. These opponents believe (or hope) that the Internet Age marks the end of intellectual property rights. They generally believe U.S. copyright laws are too expansive and do not want to see them enforced. They bring criticism against PIPA/SOPA in the hopes of blunting the effects of policies they do not like.

Other opponents of PIPA/SOPA are simply willfully blind to the current severity of the problem of online piracy and counterfeiting. For example, Andreessen et al. argue that "the [Digital Millennium Copyright Act] gives rights-holders a way to take down specific

infringing content, and it is working well."[7] Such a claim is clearly false given the level of piracy today and the fact that the DMCA only applies to domestic sites and users. For the most part, this report will not address claims made by those who refuse to recognize even basic facts, such as that online piracy is a substantial problem that hurts the U.S. economy. The interested reader can find this information in other reports.[8]

Other critics make claims about the effects of PIPA/SOPA that are simply inaccurate. Some Internet engineers claim that the measures enabled by the legislation would "break the Internet" in general or its domain name system in particular. Network engineers frequently claim that certain technologies "break" the Internet in whole or in part. These statements do not mean that the Internet itself will cease to work; they are complaints about deviations from certain narrow engineering principles, protocols, or standards that may not be widely used or even widely understood. This does not necessarily translate into any meaningful implications for the average user. For example, many Internet engineers have insisted that network address translation (NAT), a technology used in the routers that provide Internet connectivity to millions of homes and businesses, breaks the Internet by violating core principles such as the end-to-end principle and the use of globally unique identifiers. According to this critique, NAT also breaks specific protocols such as Session Initiation Protocol (SIP) used for voice-over-IP (VOIP) calling. Yet the Internet continues to thrive and users still make VOIP calls.

Finding a reasonable solution to the problem of online piracy and counterfeiting is too important to let hysterical, ideological posturing and threats influence public policy.

Policymakers should understand that no bill that targets foreign infringing sites would be acceptable to ideologically-driven advocates, including those who populate Internet standards bodies, regardless of their claims that they also want to reduce piracy. However, other critics have raised reasonable questions about aspects of the legislation, particularly of SOPA. While the countermeasures proposed in PIPA/SOPA that make it more difficult to distribute, locate, and earn revenue from foreign infringing websites should be adopted, policymakers should also listen to the legitimate concerns of stakeholders who make good-faith efforts to improve the legislation, rather than kill it. In particular, policymakers should ensure that the enforcement mechanisms in PIPA/SOPA are targeted, fair, and effective. Finding a reasonable solution to the problem of online piracy and counterfeiting is too important to let hysterical, ideological posturing and threats influence public policy. It is time for policymakers to take a deep breath and consider this issue on the basis of facts and rational argumentation.

In summary, Congress should:

- Recognize that online piracy and counterfeiting are serious problems in need of new policy solutions;
- Create new countermeasures that narrowly but aggressively target websites clearly dedicated to infringing activities, especially U.S.-directed foreign sites;
- Encourage and enable intermediaries in the Internet ecosystem to disallow the use of their services to distribute, locate, and earn revenue from online infringement;

- Demonstrate to other nations that combatting online infringement, including by blocking illegal sites, will neither "break the Internet" nor harm free speech; and

- Take into account the concerns of stakeholders who are negotiating in good faith to reduce online infringement, such as by ensuring that legislation is not overly broad or vague.

The purpose of this report is threefold: 1) to respond to the inaccurate claims that have been made about PIPA/SOPA by opponents of the legislation, particularly with regards to DNS filtering; 2) to offer an assessment of legitimate areas of concern that policymakers should address before proceeding with legislation; and 3) to propose an alternative solution to the most controversial aspect of SOPA.

Overview of the Stop Online Piracy Act (SOPA)

An overview of SOPA will help readers understand the key issues at stake. SOPA is divided into two parts. Title I provides mechanisms for Internet intermediaries to directly combat online piracy and grants immunity to Internet intermediaries that take voluntary action against sites infringing on U.S. IP. Title I also contains a section that directs the Attorney General to develop procedures and guidelines to implement this legislation. This section also directs the Register of Copyrights to report to Congress on the effectiveness of the legislation. The last section of Title I directs the U.S. Intellectual Property Enforcement Coordinator to report to Congress specific policy recommendations to deter "notorious foreign infringers." In particular, this section calls for the IP Enforcement Coordinator to identify whether the United States should prohibit certain foreign countries that appear on this list from raising capital in the United States. Title II includes a number of provisions that increase the penalties and sentencing guidelines for those convicted of illegally streaming copyrighted works, trafficking in inherently dangerous counterfeit goods (e.g. good or services for the military), and conducting foreign and economic espionage. Title II also contains a section that orders the Secretary of State and the Secretary of Commerce to direct more resources towards protecting U.S. IP rights abroad.

Although there are important differences between the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA), many of the same criticisms have been made about both bills. Some of the important differences between the two bills are in their definitions of an infringing website. PIPA defines an infringing site as one directly engaged in infringing activities or used "primarily as a means for engaging in, enabling or facilitating" infringing activities.[9] SOPA draws on the rulings from *MGM Studios v. Grokster* and the *Global-Tech Appliances, Inc. v. SEB S.A* to include not only websites directly engaged in infringing activities, but also those that promote infringement and those that are willfully blind to infringement.[10]

Most of the complaints about SOPA focus on sections 102 and 103 of Title I. Section 102 specifies enforcement actions the Attorney General can take against foreign infringing sites. This section allows the Attorney General to pursue a court order against infringing sites. Upon being served a copy of the court order, ISPs, search engines, payment processors and ad networks, would be required to take certain "technically feasible and reasonable measures" against infringing sites. Specifically, the legislation directs ISPs to block access to

infringing sites, search engines to stop serving links to infringing sites, payment processors to stop completing payment transactions from U.S. customers, and ad networks to cease displaying ads on infringing sites or on behalf of these sites.

Section 103 creates a system that facilitates the notification of payment processors and ad networks by rights holders that an infringing site is using their services. Section 103 applies to all infringing sites, both domestic and foreign, that are directed at U.S. audiences.[11] Notifications from rights holders must follow certain guidelines and include specific information so that the intermediary can identify the infringing site, establish that the site is dedicated to theft of U.S. property, and verify that the site is directed at a U.S. audience. Once notified, the payment processors and ad networks are directed to deliver the notice to the identified website. The identified website owner or operator can file a counter notification certifying that under penalty of perjury he or she "has a good faith belief that it does not meet the criteria of an Internet site dedicated to the theft of U.S. property."[12] If the website is a foreign website, the owner or operator must also consent to allowing U.S. courts jurisdiction to adjudicate whether the site is infringing. Once notified by the rights holder, the service provider is directed to suspend service to the infringing website within five days unless the website owner or operator files a counter notification. If a counter notification is filed or a service provider ignores the notification, the rights holder can pursue a court order to require the payment processors and ad networks to suspend service.

WHY CLAIMS THAT DNS FILTERING WILL BREAK THE INTERNET AND LEAD TO CENSORSHIP ARE UNJUSTIFIED

Many inaccurate claims have been made about PIPA/SOPA by opponents of the legislation. The most serious of these claims to date is that the proposed countermeasures in PIPA/SOPA, particularly the DNS filtering obligation, would "break the Internet" or otherwise harm users. This claim, which has been used by critics to rally the public, media and lawmakers to their cause, is completely unfounded and without merit. The first section of this report explores and refutes the key arguments of this claim in detail.

Overview of the Domain Name System (DNS)

One of the primary objections to PIPA/SOPA is the section of the legislation that allows the Attorney General to obtain a court order instructing Internet service providers (ISPs) to not resolve the Internet protocol (IP) address of foreign infringing websites. Specifically, SOPA states "A service provider shall take technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site (or portion thereof) that is subject to the order, including measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name's Internet Protocol address."[13] This would mean that users in the United States would not be directed to the IP address of an infringing website if they type in its domain name or click on a link in a web browser. To better understand critics' objections, a brief review of DNS follows.

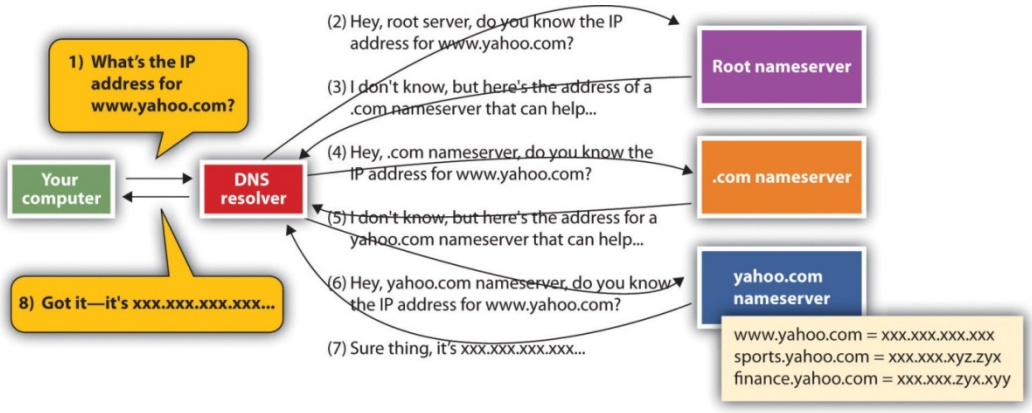

Figure 1: Resolving a DNS Query[14]

ISPs not only provide bandwidth to customers, they also typically provide a number of basic services to support Internet use. One of these services is domain name resolution which translates domain names, such as www.itif.org, into IP addresses, such as 69.65.119.60. The Domain Name System (DNS) is used by virtually every piece of software or hardware that uses the Internet, from web browsers and email applications to game consoles and streaming video devices. For example, to visit a website, a user clicks a link or enters a URL into a web browser (e.g. http://www.whitehouse.gov/omb/intellectualproperty). The web browser parses the URL to extract the domain name from the URL (e.g. www.whitehouse.gov). The user's computer then submits a request to a DNS server to resolve this domain name. ISPs provide non-authoritative DNS servers to handle queries from their users. These recursive DNS servers take a user's DNS request and, through a series of actions shown in Figure 1, determine the IP address for the domain name. The DNS server then sends a reply back to the user with the correct IP address for the domain name. All of this happens seamlessly to the user.

Claim: DNS filtering does not remove pirated content.

Some critics argue that since blocking access to a website dedicated to infringing content does not actually remove the infringing content from the Internet, it should not be done. Organizations such as the Internet Society assert that the only acceptable solution to stopping the dissemination of pirated content is to stop it at the source.[15] They take the rather narrow view that the only legitimate way to combat piracy is by stopping the production of infringing material or the posting of that material on the Internet. They argue that the distribution system for the infringing content, i.e. the Internet, should be off-limits.

This proposal is completely unworkable. This would be like arguing that domestic law enforcement should never check the contents of trucks crossing the border or cargo containers arriving at ports but instead work to eliminate the existence of contraband in the originating countries. For example, using the logic of the Internet Society, interfering with the sales or distribution of drugs is inappropriate, and government authorities should only go after the producers of drugs in foreign countries. While in both cases (drugs and online piracy) eliminating the "contraband" would be useful, it is unlikely to be achieved. As such,

a multi-pronged approach that addresses both the production and sales of illegal goods is likely to be more effective. While critics are correct that the ideal scenario would be that pirated content was never posted online, given the global nature of the Internet and poor enforcement of IP rights in many countries, this is an unlikely outcome.

Ironically, many of the voices arguing that DNS filtering does not solve the core issue, which is that pirated content is made available online, often are the same ones opposing digital rights management (DRM) technology that is created to achieve the very goal of eliminating pirated content. For example, groups like EFF have consistently opposed industry efforts to use DRM on media files or digital hardware interfaces to prevent illegal copying.[16] This underscores the fact that many of the critics of this legislation oppose all forms of IP enforcement, not just this particular bill. For example, the Internet Society also opposes government authorities seizing the domain names of criminals found guilty in their respective countries.[17]

Claim: DNS filtering is easily circumvented.

Some critics of PIPA/SOPA argue that DNS filtering is easily circumvented and thus should not be deployed. Crocker et al. make this argument in a white paper on the DNS filtering requirements in PIPA, writing "DNS filters would be evaded easily, and would likely prove ineffective at reducing online infringement."[18]

If PIPA/SOPA was enacted into law, users would have two primary means of avoiding DNS filtering.[19] First, they could use a DNS server that is not subject to the PIPA/SOPA regulations. DNS translates domain names into IP addresses. Under PIPA/SOPA, DNS servers in the U.S. would not return the IP addresses of rogue sites. To get around this, Internet users could choose to route their DNS queries to alternative DNS servers outside of U.S. jurisdiction. However, it would be a mistake to assume, as some of these network engineers have, that the average Internet user has the above-average technical skills necessary to do this. Many, if not most, consumers have low levels of computer literacy and certainly are not sophisticated enough to understand how to manipulate the DNS settings in the network configuration of their computers, mobile phones and other Internet-connected devices. Second, while users could install software on their PC to circumvent the DNS filters, the effectiveness of this method depends on the quality of the software, the willingness of consumers to install untrusted software on their computers, and how quickly users can obtain accurate information about blocked domain names.

While circumventing DNS filtering is relatively straightforward at a technical level, this does not mean that such filtering will be ineffective. First, DNS filtering will help change the perception that visiting websites enabling piracy is a legitimate activity. While some users may think nothing of clicking on a link from their favorite search engine to watch a movie online at an infringing website, these same users may think twice before using a foreign DNS server or downloading software specifically designed to circumvent federal laws. In addition, users simply may not have easy access to circumvention tools. SOPA allows the Attorney General to bring an injunction against "any entity that knowingly and willfully provides or offers to provide a product or service designed or marketed for the circumvention or bypassing of [a countermeasures in the bill]." This means that there will

not be legitimate businesses offering circumvention tools, nor will these circumvention tools be widely advertised by legitimate organizations. For example, the plug-in pages for the Mozilla Firefox or Google Chrome browsers or the app stores for the iPhone and Android devices will not be providing these tools as suggested downloads.

Finally, even if software is made available to help some users circumvent DNS filtering, it is far from certain that this software will be adopted by many users. Indeed, users have a poor history of using these types of tools in other countries where the government restricts access to certain websites. Researchers at the Berkman Center for Internet & Society at Harvard University found that "no more than 3 percent of Internet users in countries that engage in substantial filtering use circumvention tools. The actual number is likely considerably less."[20] Presumably the desire for access to essential political, historical, and cultural information is at least equal to, if not significantly stronger than, the desire to watch a movie without paying for it. Yet only a small fraction of Internet users employ circumvention tools to access blocked information, in part because many users simply lack the skills or desire to find, learn and use these tools.

So circumvention may be possible, but it is unlikely to be employed by a significant percentage of users. Some critics would say that if blocking a website is not effective all of the time, then it should not be used at all. This is the same weak argument used against virtually every type of countermeasure. Why bother locking a door, when it is possible for thieves to break it down? Why bother using metal detectors in airports, when terrorists will simply find ways to avoid detection? Why prosecute drug dealers when some will not be caught? The answer is that complex problems with no single solution benefit from multi-layered solutions. While there is no single solution that will eliminate all online piracy, there are many options that collectively can help reduce it. The standard for effectiveness should not be, as some opponents claim, elimination of all piracy. Reduction is an important goal.

Claim: DNS filtering impedes DNSSEC deployment.

A number of security problems have been found in the original DNS protocol and network engineers have been working on devising improvements to the protocol since the early 1990s. The Internet Engineering Task Force (IETF) established a working group to refine the DNS protocol, a project known as the domain name system security (DNSSEC) extensions. DNSSEC is designed to prevent certain types of attacks on the integrity of a DNS response by attaching a signature to each response. DNSSEC is currently in the process of being deployed.

Some critics say that the DNS filtering requirements in PIPA/SOPA would serve as an impediment to the deployment of DNSSEC. For example, the Internet Society argues that DNS filtering is "incompatible with DNSSEC and impedes DNSSEC deployment."[21] The Center for Democracy and Technology argues that PIPA/SOPA "could stop DNSSEC—a crucial effort to improve Internet security, over 15 years in the making—dead in its tracks."[22] The issue here is that DNS redirection is not supported by the current DNSSEC protocol. Opponents of PIPA/SOPA argue that since DNS redirection is not supported by the DNSSEC protocol, it should not be included in the legislation.

There are many problems with this argument. First, there are no technical issues with implementing DNS filtering using the current DNS protocol, which is widely used by Internet users today. In fact, many users routinely experience this type of DNS redirection while using the Internet today. For example, ISPs often use DNS redirection to monetize error traffic. When users type in a domain name that does not exist, rather than returning an error, the ISP redirects the user to a search engine to suggest possible alternatives.[23] ISPs may also use DNS redirection to communicate to users, such as to let them know of a billing issue that needs to be resolved before they can use their Internet connection. DNS providers, including OpenDNS, also use DNS redirection to protect users from harmful sites and to implement content controls. For example, parents may use OpenDNS to prevent their children from visiting adult-oriented websites or to help ensure they do not accidentally visit a malicious site. Finally, DNS redirection is used by some wireless hot spots, for example at airports, hotels, and coffee shops, to redirect users to an authentication portal to gain access to the network.[24] To be clear, DNS filtering is compatible with the current DNS protocol.

Second, there are potential ways to implement the requirements of SOPA today even for ISPs that are using DNSSEC. SOPA does not require ISPs to use DNS redirection. It only requires that ISPs prevent access to a foreign infringing site. This means that a DNSSEC server can simply decline to resolve an IP address for a domain name of a foreign infringing site by not responding to queries for that domain name. A user attempting to visit a site blocked in this manner would receive a timeout error. To make the process even more seamless, a browser extension could be created to alert users that the site is not simply inaccessible, it is blocked by order of the U.S. government. But ISPs do not even have to use DNS to block access to the site. For example, an ISP can choose to block access to a foreign infringing site through other means, such as IP blocking. Furthermore, at least for the immediate future, most DNSSEC-aware clients will not require a signed response. This means that a DNS server could return an unsigned response for a blocked site to redirect that site's traffic. None of these actions would diminish the ability to use DNSSEC to secure the DNS response of legitimate sites.

Third, even those who disagree that ISPs deploying DNSSEC have legitimate ways of implementing the requirements of SOPA cannot really complain. PIPA/SOPA states that service providers are required to take only "technically feasible and reasonable measures" to comply with government court orders. The legislation further states that a service provider is not required to "modify its network, software, systems, or facilities" to comply with these requirements.[25] This means that if DNS servers are deployed using DNSSEC, and if DNSSEC does not allow for the type of redirection or filtering specified in the legislation, ISPs would not need to take action. Thus there is no reason to suspect that ISPs would delay deploying DNSSEC because of provisions in SIPA/PIPA. If anything, to the extent that any ISPs oppose DNS filtering for ideological or technical reasons, the DNS filtering requirements in PIPA/SOPA would serve as a catalyst for ISPs to upgrade to DNSSEC since this may free them of unwanted obligations.

Fourth, there are many potential ways to improve DNSSEC to better meet the goals of the legislation. While technology should shape policy, it should not determine policy. The

U.S. policies on the Internet should not be determined by the ideological points of view of a few network engineers in the IETF. Policymakers routinely ask the private sector to design systems to meet new technical standards so as to achieve a specific policy outcome.[26] This occurs regularly in many industries, from closed captioning in TV broadcasting to emissions standards and fuel efficiency ratings in the automobile industry. DNSSEC, as with many technical standards, is not an immutable set of rules carved by God on stone tablets. Although DNSSEC has been codified in various technical documents, it continues to evolve over time as researchers propose new modifications to the standard to address various limitations.[27] The question policymakers should be asking is not whether the proposed solution is compatible with the current version of DNSSEC, but how to craft policies that best take advantage of potential improvements in the DNSSEC standard. If there are legitimate questions about how best to notify users that a non-authoritative DNS server is choosing not to resolve a particular request, then Congress should seek solutions from the private sector. If the private sector is unable to propose an acceptable solution, Congress should consider funding an NSF research grant to explore answers to this question.

Claim: DNS filtering is too broad of a tool.

Some critics have argued that DNS filtering causes "collateral damage" to legitimate websites.[28] As evidence of this, they point to the seizure of the domain name "mooo.com" by Immigration and Customs Enforcement (ICE) in February 2011. This particular domain name belonged to a free DNS hosting service that reportedly had over 80,000 subdomains. The domain was being used as part of a free DNS service that, among other things, allows people to host their own websites or other services on a sub-domain. Someone may use this service if they want to have an easy-to-remember name to access their computer remotely or to host a website. This is a cheap alternative for people who do not need or want to pay for their own domain name. For example, instead of registering the domain name "mywebsite.com" a user could use "mywebsite.mooo.com" for free. When "mooo.com" was seized by ICE, all of the users who had free sub-domains were affected by this seizure. Critics of PIPA/SOPA argue that this case demonstrates that taking action at the domain level, either through seizures or DNS filtering, is inappropriate.

To counter: first, this site was seized by U.S. law enforcement; the domain name was not blocked using the type of DNS filtering proposed in PIPA/SOPA. Second, since the registrar for the "mooo.com" domain is located in the United States, it was seized, not blocked, using existing law. Third, the domain name was seized because a subdomain of this domain was being used to distribute child pornography, not because it was being used to distribute copyright-infringing content.

Furthermore, the Department of Justice and Department of Homeland Security became aware of the error and within a few days the domain name was restored.[29] This error was unfortunate, but it was an isolated incident and one that was quickly remedied. Clearly, ICE can implement better controls to ensure that this type of mistake does not recur. To this end, the definitions used in SOPA have been revised from PIPA so as to clarify that blocking can be done at the subdomain level.[30]

Claim: DNS filtering poses security risks to users.

Opponents of PIPA/SOPA, such as the Internet Society and Crocker et al., argue that DNS filtering will "puts users at risk."[31] However there are no security risks from DNS filtering. Instead, the purported security risks for users come about only for those Internet users who begin using alternative DNS services (i.e. those individuals intent on breaking the law). Yet, as we have seen, to date there is little evidence that the average user will begin using these alternative DNS services. In fact, users will be unlikely to use an alternative DNS service precisely because of the security risks.

Moreover, DNS filtering has real security benefits for users. The illegal distribution of pirated content today is major security risk for consumers. Consumers who visit these websites put themselves at risk of becoming victims of fraud and identity theft. Rogue websites, files shared illegally on P2P networks, and software used facilitate the illegal distribution of digital content, are frequently the source of security threats. On the Internet, it is illegitimate sites that are typically the source of viruses, spyware and other malware that infect users' PCs, not legitimate sites like iTunes or Amazon.com. PIPA/SOPA would help users avoid the dark alleys of the Internet and take away the veneer of legitimacy that is conferred on these sites when legitimate businesses display ads, process payments, and provide incoming links to their sites.

PIPA/SOPA would help users avoid the dark alleys of the Internet and take away the veneer of legitimacy that is conferred on these sites when legitimate businesses display ads, process payments, and provide incoming links to their sites.

Claim: DNS filtering will fragment the global DNS namespace.

Some groups complain that DNS filtering will fragment the global DNS namespace, meaning it will cause some domain names to be accessible in one country, but not in another. For example, the Internet Society argues that DNS filtering eliminates "consistency and fragments the DNS, which undermines the structure of the Internet."[32] KC Claffy et al. of the Security and Stability Advisory Committee (SSAC) at ICANN issued a statement stating that DNS filtering can impact the "coherency or universal resolvability of the global namespace."[33] Andreessen et al. claim that DNS filtering "endangers the security and integrity of the Internet."[34]

Given that the goal of the legislation is to prevent users from reaching websites that contain infringing content, this is not an objection so much as it is a statement of fact. Neither law-abiding U.S. consumers nor U.S. innovators are hurt by a lack of access to websites dedicated to infringing. If other countries choose not to block infringing websites, then these illegal sites will be accessible to their citizens. Moreover, the universality of the DNS is overstated by some critics. This so-called "fragmenting" of the DNS happens today as DNS resolvers return different IP addresses to different users based on various factors. For example, as previously mentioned, users who subscribe to DNS redirection services such as OpenDNS will receive different responses than those who do not.

Claim: DNS filtering leads will lead to alternative DNS systems.

A position paper from the Internet Society claims that DNS filtering will lead to the creation of "'underground' DNS services and alternative domain namespaces." [35] Similarly, KC Claffy et al. make the argument that DNS filtering "may give rise to alternative name systems and/or roots, which would be destabilizing and disruptive for the Internet."[36] However, there is no evidence to suggest that a large number of Internet users are planning

to abandon the current global DNS in favor of an insecure alternative just so they can download pirated content.

First, alternative name systems exist today, and Internet users have the ability to employ these systems if they so choose.[37] Groups of organizations, individuals, and companies have created these alternative DNS systems for various technical, ideological and political reasons. However, the vast majority of Internet users do not use (or even know about) these alternative DNS systems. Moreover, these systems have had no impact on the online experience of the average user.

Second, there is no reason to expect that the average Internet user will begin using an alternative DNS system if PIPA/SOPA is enacted. No critic of PIPA/SOPA has put forth credible evidence that users will flock to alternative DNS services. As even opponents of PIPA/SOPA acknowledge, a user who chooses to use an untrusted alternative DNS services faces serious security risks.[38] Proponents of this argument are making the assumption that Internet users are willing to trade the ability to securely shop, bank, and send email so that they can download music for free that they could get for $0.99 on iTunes.

Claim: DNS filtering erodes trust in the Internet.

The Internet Society claims that "DNS filtering erodes trust in the Internet when users are no longer certain that typing www.isoc.org into a web browser will get them to the ISOC web site." The concern here seems to be that users will have less trust in the Internet if they are unable to visit sites engaged in piracy.

First, unless the website of the Internet Society is dedicated to infringing, then it will not be subject to action by the Attorney General under PIPA/SOPA. Therefore, there is no justification to claim that Internet users will not be able to visit lawful websites. Second, rather than decrease trust, DNS filtering will actually increase trust in the Internet because when users type a URL into their web browser, they will know that the site they are visiting is not a rogue site. More broadly, the countermeasures proposed in PIPA/SOPA will engender more trust on the Internet as users will be able to more easily distinguish legitimate sites from illegitimate sites and be better protected from infringing sites.

Claim: DNS filtering is a form of censorship.

Some critics of PIPA/SOPA argue that the legislation will restrict lawful free speech and is a form of censorship. Ideological critics have called the PIPA/SOPA the "first American Internet censorship system."[39] The Internet Society argues that DNS filtering "has the potential to restrict free and open communications and could be used in ways that limit the rights of individuals or minority groups."[40] Of course it could. ISPs or the U.S. government could use DNS filtering to block sites they do not like. But guns can be used by criminals to kill people too and that does not mean that we do not let the police or security guards have guns. It is not the tool of DNS blocking that is at issue, but the legal regime in which the tool is allowed to be used. Some of these opponents of PIPA/SOPA are more interested in protecting access to free illegal content than they are in protecting free speech. Yet aside from these bold claims, critics have done little to show how enforcing IP rights violates any American's First Amendment rights.

Critics of PIPA/SOPA are trying to suggest that if a user is prevented from obtaining a pirated copy of the latest Hollywood film, this is an unlawful restriction of their Constitutional rights. Human rights, including the freedom of speech, are a fundamental part of our democracy and deserve the utmost respect. But this legislation makes no attempt to regulate speech on the Internet. An individual's right to free speech is not a license to infringe on the IP rights of others. The freedom of speech does not give Internet users the right to steal digital content.[41] SOPA even begins by stating "nothing in this Act shall be construed to impose a prior restraint on free speech or the free press protected under the 1st amendment to the Constitution."[42] In addition, it is worth noting that at a packet level, DNS filtering does not stop devices on the Internet from communicating with each other. Indeed, this is exactly the argument made by opponents of PIPA/SOPA (see "Claim: DNS filtering is easily circumvented"). DNS filtering only prevents recursive DNS servers from aiding users in locating the IP address of known infringing websites.

Claim: DNS filtering will induce other nations to restrict free speech.

Critics of PIPA/SOPA are trying to suggest that if a user is prevented from obtaining a pirated copy of the latest Hollywood film, this is an unlawful restriction of their Constitutional rights.

Some opponents of PIPA/SOPA have argued that DNS filtering will encourage other countries to restrict free speech online and that DNS filtering is antithetical to a free and open Internet. The American Library Association, Consumer Electronics Association, NetCoalition, and Public Knowledge, argue that DNS filtering "may be used to justify foreign blacklists of websites that criticize governments or royalty, or that contain other 'unlawful' or 'subversive' speech."[43] The ACLU even argues that "if we adopt an overly broad online infringement takedown scheme, what will that say to the nations that frequently remove content they find objectionable, like China?"

In short, these groups are trying to equate the United States protecting its intellectual property online with authoritarian governments suppressing free speech. This criticism does not stand up to a serious analysis. This would be like arguing that when U.S. law enforcement arrests criminals, it encourages anti-democratic, totalitarian governments to use their police to repress their law-abiding citizens. Regardless of whether the United States enacts PIPA/SOPA, other countries will continue to be free to block access to websites if they so choose (and most will continue to choose to do so). However, the United States does have an opportunity to demonstrate leadership on these issues by protecting both free speech and intellectual property online. By passing this legislation, the United States can show other countries that there need not be any conflict between protecting free speech and preventing online copyright infringement. This may encourage other nations to implement stronger protections for IP, a move which would benefit the U.S. economy and boost U.S. global economic competitiveness.

POLICYMAKERS SHOULD ADDRESS LEGITIMATE CONCERNS ABOUT PIPA/SOPA

The Internet has been a powerful driver of innovation and productivity in the United States and around the world. Policymakers should always consider carefully any legislation that could impact this powerful creator of jobs and economic growth. But that does not mean the Internet should be free of the rule of law. While, as with any important legislation, stakeholders should fully evaluate the proposal and continue to refine definitions and close potential loopholes, overall the framework created by PIPA/SOPA

provides a multi-layered approach to addressing a serious problem that is a drain on the U.S. economy.

Separate Fact from Fiction

Opponents of PIPA/SOPA have issued a variety of claims about the legislation, much of it misleading or false. Some of the claims by critics of the legislation are even contradictory. For example, opponents of PIPA/SOPA argue that the legislation will be completely ineffective at stopping users from accessing pirated content, but then also argue that the legislation will hurt free speech. Critics of the legislation would have others believe that PIPA/SOPA will be useful for blocking all content *except* pirated content.

The legislation has attracted a high-profile set of opponents, from political leaders with the Tea Party and Demand Progress to technical ideologues at the Internet Society and the Electronic Frontier Foundation. Moreover, online communities have been mobilized to lobby against the legislation with dubious information about the impact of the enforcement mechanisms from a wide variety of sources ranging from tabloid blogger Perez Hilton to security consultant Dan Kaminsky.[44]

No change to PIPA/SOPA will ever satisfy those who fundamentally reject the idea that governments should have authority over the owners and operators of the networks, servers, and software that make up the Internet.

Some simply reject PIPA/SOPA because it does not fit their world view.[45] In particular, people diverge on two questions: whether intermediaries have a responsibility to enforce standards and norms online and whether IP theft is a problem deserving of government intervention. No change to PIPA/SOPA will ever satisfy those who fundamentally reject the idea that governments should have authority over the owners and operators of the networks, servers, and software that make up the Internet. These cyber-libertarian groups will reject any legislation that places responsibility on Internet intermediaries to protect intellectual property rights online. Neither will any changes to the legislation ever satisfy those who reject the ideas that IP theft is a problem and that government should do more to protect IP rights online. In fact, many of these groups would like to roll back the protections afforded to copyright holders under the Digital Millennium Copyright Act (DMCA).

The position of many of these groups is ideologically inconsistent.[46] While some may insist that they do want government to enforce IP rights on the Internet, they offer up a long list of caveats that, if included, would effectively neuter any efforts to reduce IP theft. Moreover, for many of these groups, particularly those on the left side of the political spectrum, enforcing IP theft is doing the bidding of rich corporations who should be responsible for looking out for their own profits, and not rely on the state to do so. But at the same time when these IP right holders attempt to do just that, for example by filing lawsuits against individuals who engage in massive levels of piracy, they are vilified by these liberal groups as hurting innocent Americans.

On the other hand, with regards to other Internet policy issues, these groups are dismissive of a balanced approach. For example, the same groups that reject efforts to protect IP rights online give a full-throated endorsement of heavy-handed government efforts to mandate consumer privacy regulations for the Internet regardless of the cost. In both cases moderation and clear-thinking is needed. And government actions to limit illegal activity

on the Internet are much more likely to be in the broad public interest than actions to regulate legitimate commerce to suit the needs of some advocacy groups.

Address Legitimate Concerns

Those who believe that intermediaries on the Internet should play an active role in enforcing rules of behavior and that government should do more to protect IP online may not fully endorse PIPA/SOPA, yet recognize that the general framework outlined in the legislation will provide a valuable mechanism to combat rogue sites. It is to these stakeholders that policymakers should turn for guidance to refine the legislation. In particular, policymakers should work with stakeholders to ensure that the legislation contains clear and unambiguous definitions, minimizes compliance and enforcement costs to the private sector, and creates a process that protects the rights of those who may be wrongly accused of infringement.

It is important to ensure that legislation properly protects innovation in the technology sector of the U.S. economy, especially for start-ups. A recent letter from some members of Congress argues that "venture capitalists will be hesitant to invest in new Internet-based businesses if they fear their money will be tied up in litigation."[47] To be clear, innovation and U.S. competitiveness are not dependent on the ability of U.S. businesses to infringe on intellectual property. The success of the U.S. technology industry is based on the quality of its products and services, not on how much intellectual property it can enable to be stolen from the content industry. Sites like Netflix, Hulu and iTunes have thrived not because they infringe on content, but because they offer an affordable and high-quality alternative to piracy. Yet they would thrive even more if consumers had less access to pirated content. Moreover, many start-ups face unfair competition from illegal websites operating overseas. As others have said before, it is hard to compete with free. By helping to reduce access to copyright infringing content, PIPA/SOPA can give legitimate start-ups a fair chance.

Furthermore, the argument that venture capitalists will decrease investment in Internet-based companies is weak at best. Certainly if the United States were to eliminate copyright protection for digital content, we would see a boom in investment for web-based services taking advantage of this free content. But naturally we would also see a drop off in investment (and jobs) in the content industries and the companies providing legal access to content, and a decline in the availability of quality content. Conversely, an increase in the level of enforcement of intellectual property will lead to an increase in investment in start-ups that offer legal content. Clearly a balance is needed. Given the high levels of infringing content on the Internet today and the ability of Internet intermediaries to reduce piracy, this balance needs to tilt towards more protection of content. Still it is worth considering how to refine the definitions used in PIPA/SOPA to create more certainty for investors and make clear that legitimate businesses, particularly domestic websites, will not be exposed to expensive litigation or additional liability.

It is also important to ensure that PIPA/SOPA does not impose unfair costs on legitimate businesses or expose them to unfair secondary liability. In particular, some critics argue that PIPA/SOPA would require owners and operators of user-generated content (UGC) sites to undertake onerous monitoring requirements. For example, the Center for Democracy and

Technology (CDT) argues that "Any website that features user-generated content or that enables cloud-based data storage could end up in its crosshairs. ISPs would face new and open-ended obligations to monitor and police user behavior."[48] Similarly, Gary Shapiro from the Consumer Electronics Association argues "SOPA could force tech companies to pre-screen and monitor all user comments, pictures and videos — essentially destroying social media."[49]

Once again, revising the definitions used in the legislation may help to bring confidence to a broader group of stakeholders, especially those who are not ideologically opposed to this type of legislation. Congress should make absolutely clear that only foreign sites dedicated to infringing are covered by this legislation and that these websites cannot practice willful blindness to infringing activities to avoid responsibility. Congress should also review the definitions of foreign and domestic sites to ensure that it properly categorizes websites that use a U.S.-based registrar but otherwise have their operations abroad. Moreover, efforts should be made to ensure that the notice-and-takedown provision of the DMCA is still the primary enforcement tool to combat infringement on domestic websites and that safe-harbor protection remains for DMCA-compliant sites.

USE VOLUNTARY PRIVATE SECTOR AGREEMENTS AND EXISTING LAW TO COMBAT DOMESTIC INFRINGEMENT

One of the most controversial elements of SOPA is the provision in Section 103 that allows rights holders to request a court order that would require payment processors and ad networks to terminate their services to an infringing site. One reason that Section 103 of SOPA has generated controversy is because it applies to both foreign and domestic sites. Opponents of PIPA/SOPA claim that this provision can be abused by overzealous rights holders to harm legitimate U.S. businesses. For example, Abrams et al. argue that "including a private right of action means that any rights holder can tie up a service provider in costly legal action, even if it eventually turns out to not be valid…it's not difficult to predict that plenty of legitimate startups may end up having to spend time, money and resources to deal with such actions."[50] Gary Shapiro at CEA argues that "SOPA gives Hollywood studios, as well as an unknown and potentially limitless number of plaintiffs, the ability to harass and sue lawful Internet and technology companies with little or no recourse for such websites."[51]

Many of these claims are unfounded. As described earlier, SOPA requires rights holders who want to contact payment processors and ad networks to submit detailed notifications about alleged infringing sites to ad networks and payment processors. Accused site owners and operators can file counter-notifications to defend their website. Moreover, if rights holders abuse this system they can be held liable for damages. SOPA clearly states that an entity that provides a notification "shall be liable for damages, including costs and attorneys' fees, incurred by the person injured by such misrepresentation as a result of the misrepresentation."[52] Moreover, the Internet intermediary does not face liability for its actions or inactions and there are no financial incentives to rights holders for filing unsubstantiated claims.

Still given that rights holders already have the ability to take action against domestic sites under existing U.S. law, additional legislation for domestic sites may not be necessary at this time. This is not to say that more robust enforcement mechanisms for domestic sites are not needed. Taking action under existing U.S. law is not always an efficient mechanism for enforcement. After all, creating a new website only takes a few minutes; obtaining a court order against an infringing site may take weeks or more.[53] It may be faster and more efficient for Internet intermediaries to work cooperatively to address this issue. To that end, policymakers should encourage the private sector to evaluate where it can make new commitments to better enforce intellectual property rights online through self-regulatory efforts. Specifically, policymakers should evaluate whether a multi-stakeholder approach would be better than legislation for addressing the remaining gaps in online IP enforcement for domestic sites.

The Internet depends on the multi-stakeholder model of self-governance, and Internet intermediaries have an important role to play in preventing infringement. Many Internet intermediaries, including virtually all payment processors and ad networks, already have policies in place that prohibit using their services for illegal purposes. However, a multi-stakeholder agreement might create a more effective process for intermediaries to adhere to their own stated policies and better enforce IP rights. For example, while Section 103 of SOPA would create a system to facilitate notification by rights holders to payment processors and ad networks, such a system could also be created through a voluntary joint-industry agreement. Whether it is through legislation or a self-regulatory process, there should be a system in place so that content owners can easily notify ad networks and payment processors when they identify an infringing site.

A voluntary agreement will also negate some of the concerns about due process.[54] Service providers can already choose who they want to do business with. Most service providers already have terms of service that prohibit the use of their services for illegal purposes. If a service provider receives a notice and decides that its customer is violating the terms of service, it can suspend its customer. Streamlining and standardizing this process will benefit all parties. For example, the private sector, in consultation with consumer-interest groups, could develop industry-wide guidelines for determining whether a site is dedicated to infringing. In addition, efforts could be made to make the process and actions taken by Internet intermediaries transparent to the public, such as by creating a public website to report on enforcement actions.

In one year, policymakers should evaluate if the private sector has taken sufficient action to effectively address the current set of problems. They should also evaluate if there are remaining gaps in enforcement for infringing sites, if fair use is properly protected and if there are liability risks for Internet intermediaries who take action against domestic infringing sites. It also may be necessary to develop additional countermeasures to address the problem of counterfeit goods sold from domestic sites.

The technology industry does have a track record of working collaboratively with the content industry to develop self-regulatory programs that better protect IP rights online. For example, in 2007, tech companies and media companies worked together to develop

principles for protecting intellectual property of content on user-generated content sites.[55] In July 2011 the content industry and ISPs announced the agreement of a jointly-developed graduated-response system to alert U.S. Internet users about copyright infringement.[56] These are models of effective anti-piracy measures that are both pro-consumer and pro-economy. This would also build on previous cooperative measures such as DNS blacklists which have been widely used since the late 1990s to combat spam.[57]

CONCLUSION

While this legislation could still be improved, the process would be better served if opponents would offer constructive criticism of the legislation rather than heated rhetoric and fear-mongering. To the extent that there are problems with the definitions in the legislation, critics should suggest alternative language to ensure that only those sites dedicated to infringing are covered by the bill. To the extent that there are legitimate concerns about Section 103, Congress should either revise the language to address concerns or encourage the private sector to develop a joint agreement to address this issue.

ISPs, search engines, payment processors, and ad networks are all key contributors to the vibrant Internet economy, and each must do its part to protect intellectual property.

To the credit of the authors of the legislation, many critics of PIPA/SOPA find something about the legislation that they like. In particular, there seems to be an emerging consensus that cutting off the source of revenue to rogue websites should be part of the solution. However, Congress should not stop there. It is clear that a comprehensive solution is needed to address this complex problem. It is not enough merely to cut off funds to rogue sites from payment processors and advertising networks or simply to engage in more international negotiations to promote the protection of intellectual property abroad. The various mechanisms in PIPA/SOPA, combined with other existing enforcement mechanisms such as domain name seizures, notice and takedown and three-strikes policies by ISPs, will help to diminish the impact of piracy on U.S. workers, U.S. consumers, and the U.S. economy.

Is PIPA/SOPA the last word on improving copyright enforcement online? Of course not. Even if the legislation is enacted, stakeholders will need to continue to monitor the effectiveness of existing measures and adapt to changing conditions. In addition, other measures will need to be pursued outside of Congress. This includes working to achieve better international collaboration and respect for copyright and taking trade enforcement actions. International institutions such as ICANN can also strengthen the rules related to registration of domain names to help root out bad actors and improve security online.

ISPs, search engines, payment processors, and ad networks are all key contributors to the vibrant Internet economy, and each must do its part to protect intellectual property. Some are already taking important steps. In fact, some intermediaries have reported that they already spend large sums of money protecting intellectual property rights online, and their financial interests must be balanced against those of IP rights holders.[58] But more can and should be done. Copyright enforcement is necessary for a healthy Internet ecosystem, and it should not pit the content industry against tech companies. Ideally all stakeholders should come together to find fair solutions that both protect the rights of IP rights holders and respect the unique challenges of the Internet economy.

ENDNOTES

1. David Price, "An Estimate of Infringing Use of the Internet," Envisional (2011), http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.
2. Ruben Cuevas et al. "Is Content Publishing in BitTorrent Altruistic or Profit-Driven," ACM CoNEXT 2010 (November 2010), http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/11-Cuevas.pdf.
3. "Traffic Report: Online Piracy and Counterfeiting," MarkMonitor, January 2011.
4. Gautham Nagesh, "ICE's Morton aims to pull plug on piracy," *The Hill*, September 23, 2011, http://thehill.com/business-a-lobbying/183453-ices-morton-aims-to-pull-the-plug-on-piracy.
5. Daniel Castro, "Targeting Websites Dedicated to Stealing American Intellectual Property," Information Technology and Innovation Foundation, February 12, 2011, http://www.itif.org/files/2011-coica-testimony.pdf.
6. Corynne McSherry, "Sopa: Hollywood Finally Gets A Chance to Break the Internet," (blog post, Electronic Fronteir Foundation, Washington, D.C., October 2011), https://www.eff.org/deeplinks/2011/10/sopa-hollywood-finally-gets-chance-break-internet.
7. Marc Andreessen et al., Letter to Congress Regarding S. 968 (June 23, 2011).
8. See, for example, Daniel Castro, Richard Bennett and Robert Atkinson, "Copyright Policy, Creativity and Innovation in the Internet Economy," Information Technology and Innovation Foundation (October 27, 2010), http://www.itif.org/files/2010-noi-piracy.pdf
9. PROTECT IP Act of 2011, S. 968, 112th Congr. (2011).
10. Global-Tech Appliances, Inc., et al. v. SEB S. A., No. 10-6, slip op., U.S. Supreme Court (May 31, 2011), http://www.supremecourt.gov/opinions/10pdf/10-6.pdf and Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd., et al., 545 U.S. (2005), http://www.copyright.gov/docs/mgm/opinion.pdf.
11. Evidence of being a U.S.-directed site include whether the site provides, or intends to provide, goods or services to U.S. users, does not take "reasonable measures" to prevent its goods or services from being obtained in or delivered to the United States, and displays or bills prices for goods or services in U.S. dollars.
12. Stop Online Piracy Act, H.R.3261, 112th Cong. (2011).
13. Stop Online Piracy Act, H.R.3261, 112th Cong. (2011).
14. Image credit: John Gallaugher, Information Systems: A Manager's Guide to Harnessing Technology (Flat World Knowledge), http://www.flatworldknowledge.com/pub/1.0/information-systems-manager's-/.
15. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," September 15, 2011, http://www.isoc.org/internet/issues/docs/dns-filtering_20110915.pdf.
16. See for example Fred Von Lohmann, "Year-end 2006, Darknet Assumptions = True," Electronic Frontier Foundation, December 29, 2006, https://www.eff.org/deeplinks/2006/12/year-end-2006-darknet-assumptions-true.
17. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering."
18. Steve Crocker et al. "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," May 2011, http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.
19. DNS can also be bypassed by entering the IP address into the web browser directly. This approach would not be successful if the unlawful content is hosted in a shared web server using virtual domains. Virtual domains allows a number of domain names to share a common IP address, and relies on the fact that web transactions send the domain name from the user's browser to the web server as typed in the browser window. When a user types "http://www.example.com" in his or her web browser, for example, the web server receives a message containing "www.example.com," which is used to distinguish it from other domains sharing an IP address with it. If the user enters an IP address, this feature is inoperative. Similar approaches are used in other parts of the Internet for various services.
20. Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris and John Palfrey, "2010 Circumvention Tool Usage Report," The Berkman Center for Internet & Society (October 2010), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

21. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," 3.
22. Leslie Harris and David Sohn, Letter from Center for Democracy and Technology to Members of the U.S. Senate, September 23, 2011, http://cdt.org/files/pdfs/CDT-PIPA_letter_sept_2011.pdf.
23. Nicholas Weaver, Christian Kreibich and Vern Paxson, "Redirecting DNS for Ads and Profit," Proceedings of the 20th USENIX Security Symposium's Workshop on Free and Open Communications on the Internet (FOCI '11), San Francisco, California, August 2011, http://www.icir.org/christian/publications/2011-foci-dns.pdf.
24. Some wireless hot spots use other forms of redirection such as HTTP redirection.
25. Stop Online Piracy Act, H.R.3261, 112th Cong. (2011).
26. Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review," Information Technology and Innovation Foundation (2011), http://www.itif.org/files/2011-impact-regulation-innovation.pdf.
27. For example, NSEC3 was introduced in March 2008 to modify how the authenticated denial of existence would work. "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence," (proposed standard, Network Working Group), http://tools.ietf.org/html/rfc5155.
28. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," 3 and Crocker et al. "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," 13.
29. Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *InformationWeek*, February 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/229218959.
30. See definition of domain name in Stop Online Piracy Act, H.R.3261, 112th Cong. (2011): "The term "domain name" has the meaning given that term in section 45 of the Lanham Act (15 U.S.C. 1127) *and includes any subdomain designation using such domain name as part of an electronic address on the Internet to identify a unique online location.*" The italicized portion of the text reflects an addition to the definition in SOPA.
31. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," 3 and Crocker et al. "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," 10.
32. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," 3.
33. ICANN Security and Stability Committee, "DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System," June 14, 2011, http://www.icann.org/en/committees/security/sac050.pdf.
34. Marc Andreessen et al., Letter to Congress Regarding S. 968 (June 23, 2011).
35. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering," 3.
36. ICANN Security and Stability Committee, "DNS Blocking: Benefits Versus Harms."
37. See for example, New.net, Public-Root and 42registry.
38. See for example, Crocker et al. "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," 10.
39. See American Censorship Day, http://americancensorship.org/.
40. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering."
41. For more on this, see Floyd Abrams, Letter to Chairman Patrick Leahy, May 24, 2011, http://www.mpaa.org/Resources/30a27707-9da9-4cf3-b642-4fb949969102.pdf.
42. Stop Online Piracy Act, H.R.3261, 112th Cong. (2011).
43. Letter from Public Knowledge et al. on "S. 3804, Combating Online Infringement and Counterfeits Act (COICA), September 27, 2010, http://www.publicknowledge.org/files/docs/JointLetterCOICA20100929.pdf.
44. Perez Hilton Blog, "Congress Working to Censor The Internet Very Soon…Starting Today!" November 16, 2011, http://perezhilton.com/2011-11-16-congress-wants-to-censor-the-internet.
45. Robert D. Atkinson, "Who's Who in Internet Politics: A Taxonomy of Information Technology Policy," Information Technology & Innovation Policy (October 2010), http://www.itif.org/files/2010-digital-politics.pdf.
46. Robert D. Atkinson, "Network Policy and Economic Doctrines," *2010 Telecommunications Policy Research Conference (TPRC)*, October 2010, http://www.itif.org/files/2010-network-policy.pdf.

47. Anna G. Eshoo et al., Letter to Chairman Smith and Ranking Member Conyers on H.R. 3262, November 15, 2011.
48. Jon Healey, "Technology: A bipartisan attempt to regulate the internet?" *Los Angeles Times*, October 26, 2011, http://opinion.latimes.com/opinionla/2011/10/technology-a-bipartisan-attempt-to-regulate-the-internet.html.
49. Gary Shapiro, "Smith bill could destroy social media." My San Antonio, November 17, 2011, http://www.mysanantonio.com/news/article/Smith-bill-could-destroy-social-media-2272768.php.
50. Jonathan Abrams, et al., "Letter to Members of U.S. Congress regarding PIPA," *Los Angeles Times*, http://opinion.latimes.com/files/entrepreneurs-worried-about-pipa.pdf.
51. Gary Shapiro, "Smith bill could destroy social media."
52. Stop Online Piracy Act, H.R.3261, 112th Cong. (2011).
53. See, for example, the recent seizure of domain names by Chanel. Nate Anderson, "Federal Judge Orders Google, Facebook to Disappear Hundreds of Sites," Ars Technica, November 29, 2011, http://www.wired.com/threatlevel/2011/11/chanel-trademark/.
54. Jason Mazzone, "The Privatization of Copyright Lawmaking," TorrentFreak, November 12, 2011, http://torrentfreak.com/the-privatization-of-copyright-lawmaking-111112/.
55. "Internet and Media Industry Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights," news release, October 18, 2007, http://www.ugcprinciples.com/press_release.html.
56. Center for Copyright Information, "Music, Movie, TV, and Broadband Leaders to Curb Online Content Theft," news release, July 7, 2011, http://www.copyrightinformation.org/node/704.
57. See DNSBL Information at http://www.dnsbl.info/.
58. *Stop Online Piracy Act of 2011: Hearings on H.R. 3261, Before the House Comm. on the Judiciary*, 112th Cong. (2011). Statement of Katherine Oyama, Copyright Counsel, Google Inc., http://judiciary.house.gov/hearings/pdf/Oyama%2011162011.pdf.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson, Richard Bennett and Morgan Reed. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, OR ONLINE AT WWW.ITIF.ORG.