



**Testimony of Katherine Oyama, Copyright Counsel, Google Inc.  
Before the House of Representatives Committee on the Judiciary  
Hearing on H.R. 3261, the Stop Online Piracy Act  
November 16, 2011**

Chairman Smith, Ranking Member Conyers, and members of the committee.

Thank you for the opportunity to testify on the recently introduced Stop Online Piracy Act (“SOPA”), H.R. 3261.

During these difficult economic times, we are proud to represent and be part of one of the fastest growing sectors of the U.S. economy, with a strong record of job-creation and innovation. The Internet today remains one of the few bright lights of our economy.

In 2010, for example, Google alone generated \$64 billion of economic activity for American businesses and non-profits. In addition, a recent McKinsey Global Institute report<sup>1</sup> found that the Internet represents 15 percent of U.S. Gross Domestic Product (“GDP”) growth in the last five years. According to the report, if Internet consumption and expenditure were a sector, its contribution to GDP would be greater than energy, agriculture, communication, mining, or utilities. In addition, the Internet industry has increased productivity for small and medium-sized businesses by 10 percent. And Internet advertising alone is responsible for \$300 billion of economic activity in the United States, representing 2.1 percent of U.S. GDP.<sup>2</sup>

The Internet industry has serious concerns with SOPA. Earlier this week, nine leading Internet companies (AOL, eBay, Facebook, Google, LinkedIn, Mozilla, Twitter, Yahoo!, and Zynga) sent a letter to the Committee, echoing concerns voiced by industry associations, entrepreneurs, small business owners, librarians, law professors, venture capitalists, human rights advocates, cybersecurity experts, public interest groups, and tens of thousands of private citizens. That letter is attached to this testimony, and my prepared testimony has been endorsed by the Consumer Electronics Association, the Computer & Communications Industry Association, TechNet, and NetCoalition —associations that sought to testify directly today and represent a diversity of concerns with legislation that could impact the innovation and growth of the Internet.

We support SOPA’s stated goal of providing additional enforcement tools to combat foreign rogue websites that are dedicated to copyright infringement and counterfeiting. Unfortunately, we cannot support the bill as written, as it would expose law-abiding U.S. Internet and technology companies to new uncertain liabilities, private rights of action, and technology mandates that could require monitoring of web sites and social media. Moreover, we are concerned that the bill sets a precedent in favor of Internet censorship and could jeopardize our nation’s cybersecurity. In short, we believe the bill, as

---

<sup>1</sup> McKinsey Global Institute, “Internet Matters,” (May 2011), *available at*: [http://www.mckinsey.com/mgi/publications/internet\\_matters/pdfs/MGI\\_internet\\_matters\\_full\\_report.pdf](http://www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf).

<sup>2</sup> John Dreighton and John Quelch, “Economic Value of the Advertising-Supported Internet Ecosystem,” (June 2009) *available at*: [http://www.iab.net/insights\\_research/530422/economicvalue](http://www.iab.net/insights_research/530422/economicvalue).

introduced, poses a serious threat to our industry's continued track record of innovation and job-creation.

While we have serious concerns with SOPA as written, we look forward to working with the Committee to find focused mechanisms that effectively target foreign rogue sites. Already, Google and other companies are engaged in voluntary, industry-led efforts to attack the problem. As detailed below, we believe that legislation guided by common sense principles and focused on eliminating the financial incentives for rogue sites – while avoiding collateral damage – would receive wide support from the technology sector.

### **The Problem of Foreign Rogue Sites**

The problem of rogue foreign sites is a real one, and not just in the context of copyright infringement and distribution of counterfeit goods. In considering what Congress can do about them, however, it is important to keep two things in mind.

First, though foreign rogue sites are a real problem, they represent a very tiny portion of what the Internet is all about. Overall, Internet technologies have delivered unprecedented benefits to citizens and businesses (including copyright and trademark owners) in the U.S. and around the world.

Second, the Internet remains a very dynamic environment, and those who operate foreign rogue sites are becoming increasingly sophisticated about evading detection and enforcement. Google itself battles every day against bad actors who target Gmail for account hijackings, Search for web spam manipulation, and AdWords for fraud. Stopping foreign rogues is a serious technical undertaking, and we have hundreds of employees focused on the problem.

In light of these two facts about rogue sites, any legislation in this field should be carefully crafted, narrowly focused, and clearly targeted at the foreign rogue sites. Casting the net too broadly threatens collateral damage to legitimate businesses and activities online, while letting the rogues wriggle free.

The good news here is that, working with Intellectual Property Enforcement Coordinator (“IPEC”) Victoria Espinel, U.S. companies have been working hard on voluntary, industry-led solutions to these problems. While these efforts are not the primary focus of these hearings, we would be happy to provide you with more details about those efforts, which focus on Internet Service Providers (“ISPs”), payment processing, and advertising services.

### **Our Concerns about SOPA**

Turning to SOPA, let me begin with a concrete example of how the bill might work in practice. Imagine you are a small business that has established a new website that “enables or facilitates” (to use the language of Section 103) other small businesses to sell clothing and accessories. Let's further imagine that 99 percent of your sellers are entirely legitimate, but that, unbeknownst to you, one seller has recently begun selling counterfeit handbags and T-shirts that parody famous copyrighted logos. Finally, let's imagine that you fully comply with all the laws that govern Internet intermediaries, including the “notice-and-takedown,” “repeat infringer,” and other requirements of the Digital Millennium Copyright Act's (“DMCA”) safe harbors.

This is the kind of company that is the model of an innovative American startup, and can hardly be called a foreign rogue site. Yet, under SOPA, your entire site could be deemed to be “dedicated to theft” because, unbeknownst to you, a “portion” of your site is being “primarily operated for” unlawful activity

by one of your sellers. Anyone who believes they have been harmed by this single bad seller (not just the owners of the specific copyrights or trademarks being infringed) can send a “termination notice” to the payment processors that you and your other subscribers rely on. The complaining party need never have made any effort to contact you to resolve the issue or to avail themselves of your DMCA “notice-and-takedown” procedures.

The first you would hear about this is when your advertising and payment services forward the allegation of infringement. You would be in the difficult position of having to judge whether the handbags are counterfeit and whether the T-shirts are protected by fair use. You would have to hire lawyers and investigators. If you fail to send a counternotice within five days, you could find your site effectively out of business, and the small businesses that rely on your services could find themselves cut off from their customers.

All of this could happen to your business without any prior due process or court involvement. Even if you do provide a counternotice to your payment and advertising services, those providers remain free under Section 104 of the bill to ignore it. And even if they do accept your counternotice, the complainant can still bring a court action directly against you. Given the breadth of the definition of “site dedicated to theft,” you may find yourself hard-pressed to defend yourself, notwithstanding your good faith efforts. Facing these potential risks, perhaps you would think twice about establishing your business in the first place.

This example is meant to highlight a number of concerns that we have with SOPA as introduced. These concerns can be organized into six categories: (1) SOPA Would Conflict with and Undermine the DMCA; (2) SOPA Puts Law-Abiding U.S. Companies in Jeopardy; (3) SOPA Imposes New, Uncertain Technology Mandates on U.S. Companies; (4) SOPA Exposes U.S. Payment Network Providers and Internet Advertising Services to Private Legal Action; (5) SOPA Will Create Security Risks to Critical U.S. Infrastructure; and (6) SOPA Violates the First Amendment and Authorizes Government Censorship of the Internet.

### **SOPA Would Conflict with and Undermine the DMCA**

The DMCA’s safe harbor provisions are a critical part of the legal foundation that has made the U.S. Internet industry the most successful in the world. Since its enactment in 1998, the DMCA has served as the “rules of the road” where copyright is concerned for virtually every major Internet company, including Google, Yahoo!, Amazon, eBay, Facebook, and Twitter. The safe harbor approach has also served as a model for our trading partners abroad, helping to create an international legal environment that allows copyright holders to enforce their rights and U.S. Internet innovators to thrive in our increasingly global markets.

The DMCA carefully balances the competing interests of different stakeholders. It protects the privacy of Internet users by making clear that Internet companies do not need to monitor their activities in order to qualify for the safe harbor. It protects copyright owners by providing them a quick and efficient means to remove infringing material from the Internet by notifying Internet companies. It protects website operators and others posting content on the Internet by targeting the relief at the infringing content (rather than against entire sites) and by providing a mechanism for counter-notification.

SOPA undermines the DMCA safe harbors in three important ways.

First, the bill creates uncertainty about whether court orders issued against “foreign infringing sites” and “sites dedicated to theft” might disqualify an online service provider from the DMCA safe harbors. Any

uncertainty on this question represents a serious threat to virtually every Internet company, reaching far beyond the intermediaries identified in the bill.

For example, if companies like Google, Facebook, and Twitter were to lose their safe harbor protections for the links shared by their users, each would have little choice but to affirmatively monitor all user activities looking for “bad links.” The burden and invasion of user privacy that this would represent is precisely what Section 512(m) of the DMCA sought to avoid. The very practice of linking on which the Web has been built could be imperiled. This concern led the Senate to include a savings clause in the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (“PROTECT IP”), S. 968, that attempts to clarify that service providers that receive and act on court orders should not be punished by having their DMCA safe harbors placed in jeopardy. A provision of this sort is crucial to preserving the business certainty created by the DMCA.

Second, SOPA defines “foreign infringing site” and a site “dedicated to theft of U.S. property” in a manner that sweeps in sites (foreign and domestic) that comply fully with the DMCA’s safe harbor provisions. The definitions make no mention of DMCA compliance as a defense, and rightsholders are likely to argue that because the DMCA safe harbors are merely limitations on remedies, sites that comply with their requirements are nevertheless infringers within the meaning of SOPA’s definitions. Accordingly, despite “playing by the rules,” DMCA-compliant sites would face the extraordinary remedies created by SOPA. These risks could force Internet companies to take a completely different approach to hosting and linking to third-party content.

Third, a site can also be declared to be “dedicated to theft of U.S. property” if it fails to confirm “a high probability” that the site has been used for infringing activities. This is true whether or not the “failure to act” would itself violate existing law. And because some rightsholders will likely contend that there is a “high probability” that all social networking and user-generated content sites are used for infringement by some users, this provision could effectively force those site operators to actively monitor their users’ activities, contrary to Section 512(m) of the DMCA.

In short, SOPA as written cannot peacefully coexist with the DMCA safe harbors. By creating new legal uncertainty for Internet companies, SOPA will significantly deter current and future Internet businesses from investing in new ventures. If SOPA were the law in 2005, it may well have been that YouTube’s founders and initial venture capital investors would have opted to do something else, discouraged by the new quagmire of legal uncertainty created by the conflicts between SOPA and the DMCA. Had that happened, we would never have come to realize what a powerful platform YouTube could be for commerce and democracy.

### **SOPA Puts Law-Abiding U.S. Companies in Jeopardy**

Foreign rogue sites flout U.S. laws by operating offshore, beyond the reach of U.S. courts. The definitions in SOPA, however, target not only foreign rogue sites, but also law-abiding U.S. companies. There is no reason that U.S. companies that are playing by the rules and subject to the jurisdiction of U.S. courts should be targeted by legislation aimed at foreign rogue sites.

The definition of “site dedicated to theft” puts law-abiding U.S. companies in jeopardy in four ways. First, by reaching sites that “enable or facilitate” unlawful activity, the definition needlessly reaches beyond existing law, which already incorporates appropriate concepts of secondary liability, such as inducement, contributory infringement, and vicarious liability. Second, the “unit of analysis” for purposes of the definition focuses not on the site as a whole, but rather any “portion thereof.” In other words, the legislation appears to target sites even where only a small portion (or even a single page) is

used for unlawful purposes. Third, as noted above, the definition can be read to sweep in sites that are completely compliant with their obligations under the DMCA. And finally, the definition includes sites that fail to confirm a “high probability” that the site is being used for unlawful activity – a standard that has never, by itself, created liability for a site operator.

As mentioned at the outset, Section 103’s “notice-and-terminate” regime also exposes law-abiding U.S. companies to substantial risks by offering anonymous “trolls” a simple avenue for cutting off legitimate companies from payment processing and advertising services. As those familiar with the antics of anonymous Internet pranksters and copyright trolls will appreciate, individuals pursuing malicious agendas can fabricate “termination notices” that intermediaries are required to comply with unless they receive a counternotice within five days. Legitimate sites, both foreign and domestic, trying to defend themselves against a barrage of illegitimate termination notices will have little recourse against anonymous trolls who may themselves be “foreign rogues,” impossible to identify and too impecunious to pay any judgments. Advertising and payment networks, moreover, are not in a position to sort the valid from invalid notices, since the statute stipulates that they “shall” terminate services within five days, or else face the possibility of legal action themselves.

### **SOPA Imposes New, Uncertain Technology Mandates on U.S. Companies**

SOPA could expose U.S. Internet companies and financial services firms to technology mandates. The Attorney General or private parties can call upon federal judges to second-guess technological measures used to block access or terminate services to Internet sites.

Under Section 102, a service provider (which under the bill’s definition can include university networks, libraries, and private businesses, as well as large commercial ISPs) is required to take “technically feasible and reasonable measures designed to prevent access” to illegal sites, including, *but not limited to*, measures designed to prevent the domain name of the infringing site from resolving to that domain name’s Internet Protocol address (“IP address”). It is not clear what other steps a service provider must take, and presumably the Attorney General and a judge can require a service provider to create new technology solutions to block access to illegal sites. The bill fails to specify what these steps might entail. The bill’s caveat that a service provider does not have to “modify its network, software, systems, or facilities” does not clarify the issue, as it is preceded by the words “other than as directed under this subparagraph.”

Similarly, an Internet “search engine” is required to take “technically feasible and reasonable measures” to prevent an illegal site from being served as a direct hypertext link. In an era where search results are evolving rapidly beyond “ten blue links,” it is not clear what this obligation might require. For example, search engines today routinely offer “previews” of web pages as part of their search results. Does a search engine have to parse every link on a web page to determine whether the page includes a link to a “foreign infringing site” before displaying it as a preview? Search engines presumably will have to await the outcome of litigation with the Attorney General in order to find out the answer to this and other questions as search results continue to evolve. This is a recipe for legal uncertainty that will chill and slow legitimate innovations in search.

Payment networks and Internet advertising services are also required to take “technically feasible and reasonable measures” to terminate providing their services to sites targeted by the bill. These law-abiding U.S. service providers will also be left to wonder what their obligations might be, until they are hauled into court and their efforts second-guessed by federal judges. Under Section 103, these court actions are not limited to the Attorney General -- private “qualifying plaintiffs” can ask the court to impose additional technology mandates on payment processors and ad networks.

## **SOPA Exposes U.S. Payment Network Providers and Internet Advertising Services to Private Legal Action**

Section 103 of SOPA threatens U.S. payment and advertising networks, which have themselves violated no laws, with expensive civil litigation at the hands of a broad array of private entities. If a private “qualifying plaintiff” believes that a payment or advertising network has not complied with its obligations under SOPA, it can obtain a default judgment against the site in question and initiate a “show cause” proceeding against the payment network provider or advertising service. In addition to requiring additional technical measures, the court can impose monetary sanctions.

The “qualifying plaintiff” entitled to initiate the Section 103 process is not limited to the owner of a copyright or trademark infringed by or through a site “dedicated to the theft of U.S. property.” Instead, the term “qualifying plaintiff” appears to mean any holder of an intellectual property right, so long as the holder (not the right) is “harmed” by the activities that cause the website to fall within the definition of a site dedicated to theft of U.S. property. Thus, under this broad definition, it is conceivable that a celebrity could rely on a right of publicity or ownership of unrelated copyrights to target a site with a “termination notice” and subsequent legal action. This is not merely a hypothetical concern – Perfect 10, a litigious pornography vendor, has asserted copyrights and rights of publicity *that it does not own* in lawsuits against Internet companies. SOPA’s broad and imprecise definition of “qualified plaintiff” is an invitation to similar litigants in the future.

The only affirmative defense specified for the “show cause” proceeding is that the payment network provider or advertising service lacks “the technical means to comply with this subsection without incurring an unreasonable economic burden,” a highly ambiguous standard. A payment or advertising service would presumably be required to provide expert testimony, subject to cross-examination, to establish that it had met its burden under this standard. The expense of defending these actions will lead some payment and ad networks to “over-terminate” when receiving notices from qualifying plaintiffs. Others may be forced into monetary settlements in order to avoid the expense of defending these actions, even where they are confident of prevailing on the merits.

## **SOPA Will Create Security Risks to Critical U.S. Infrastructure**

SOPA requires ISPs to take “technically feasible and reasonable measures designed to prevent access by its subscribers...to the foreign infringing site..., including measures designed to prevent the domain name of the ...site...from resolving to the domain name’s Internet Protocol address.”

Leading Internet security engineers agree that the proposed measure to block the domain name from resolving to the IP address has several deficiencies: (1) It is easily circumvented by the user or foreign web site; (2) it thwarts a 10-year effort to roll out new security protocols in the Domain Name System (“DNS”), called the Domain Name System Security Extensions (“DNSSEC”), which are designed to prevent an ISP (or anyone else) from interfering with a secure connection between the user and a desired website (this security system was implemented to make sure that when a user seeks to go to wells Fargo.com, the user can be assured that he or she will go to the real Wells Fargo website, rather than a phishing site); and (3) it introduces a critical new vulnerability to our Internet infrastructure as users inevitably turn to offshore, untrustworthy DNS providers as an alternative to the censored DNS services offered by their ISPs.

SOPA’s provisions aimed at technologies that circumvent measures taken by service providers to block “foreign infringing sites” do not solve these problems. Every modern computer operating system

includes simple mechanisms that allow users to redirect their browser to use different servers for DNS resolution. Accordingly, SOPA's provisions in this regard are not likely to prevent users from learning how to evade DNS blockades imposed by their ISPs, and thereby potentially compromise the security of their computers and our Internet infrastructure.

### **SOPA Raises Serious First Amendment Concerns**

In the face of efforts by the U.S. to ensure that the Internet remains a vibrant platform for democratic free expression, SOPA sets a troubling contrary precedent. The bill envisions agents of the federal governments ordering ISPs and search engines to “disappear” foreign web sites from the Internet.

Many rightsholders have complained that China's leading search engine, Baidu, does not do enough to combat piracy. Imagine what China's response would be if U.S. ISPs were to block Baidu at the behest of the federal government – doubtless China would point to this action to justify their own censorship regime. The bill's proposed DNS remedy will encourage other countries to use DNS manipulation and site blocking to enforce a range of domestic policies, potentially fragmenting the global Internet. The bill's requirement on search engines to censor search results also sets a dangerous precedent. For years, search engines have been pushing back against foreign governments that have sought to limit the universe of information retrieved through Internet searches. SOPA as written would undercut the efforts of search engines to resist those foreign censorship demands.

SOPA raises serious First Amendment concerns for U.S. citizens, as well. The prospect of ISPs and search engines “disappearing” entire sites when they have violated no U.S. law (but only “facilitated” unlawful acts of third parties) raises serious concerns. Those concerns are exacerbated because SOPA permits these sanctions against sites when unlawful activities are limited only to a portion of the site.

On April 6, 2011, this Committee heard testimony from Floyd Abrams with regard to the First Amendment implications of action in this area. Although nominally supporting the notion that action might be permissible in certain circumstances, he made it abundantly clear that the constitutionality of a bill depended on very tight drafting of the definition of an infringing website: “First, any legislation has to be narrowly drafted, really narrowly drafted, so it only impacts websites, domains, that are all but totally infringing.”

In response to a question from Representative Conyers, Mr. Abrams responded: “I mean, if you have a court and the court says *this whole site*, at this moment, as it is today, *this whole site is an infringing site*, and you get a court order to that effect and you serve it on ISPs, it seems to me perfectly constitutional...” (emphasis added) Whether or not one agrees that this standard would be constitutional, SOPA does not meet this standard.

Earlier this month, Mr. Abrams sent a follow-up letter to members of the Committee. In it, he admits that “[w]hen injunctive relief includes blocking domain names, the blockage of non-infringing or protected content may result.” While Mr. Abrams is of the view that the censorship of some legitimate speech can be squared with the First Amendment, it is worth noting his admission that protected speech is necessarily caught by the approach contained in Section 102. Other First Amendment scholars are not as sanguine about the bill as Mr. Abrams.

### **Toward a Consensus Approach to Fighting Foreign Rogue Sites**

In raising these reservations about SOPA as introduced, we do not mean to suggest that there is nothing more that can be done to combat copyright infringement, counterfeiting, and other unlawful activity

online. In fact, the technology and payment processing community have long engaged in efforts above and beyond the requirements of the law to combat copyright infringement and counterfeiting online.

### ***Google's Efforts to Battle Copyright Infringement and Counterfeiting***

Speaking for Google, we have been actively tackling these problems, both on a unilateral basis, and in conjunction with collaborative efforts led by IPEC Victoria Espinel.

First, and most importantly, Google works closely with rightsholders to make authorized content more accessible on the Internet. The only long-term way to beat piracy online is to offer consumers more compelling legitimate alternatives. We are committed to being part of that solution. For example, YouTube is now monetizing for content owners over three billion video views per week. YouTube creates revenue opportunities for more than 20,000 partners, and record labels are now making millions of dollars a month on the site. Hundreds of YouTube users make six figures a year. Today over 2,000 media companies – including every major U.S. network broadcaster, movie studio, and record label – use the copyright protection and monetization tools that YouTube offers, and a majority of them choose to monetize rather than block their content online. We also help content creators make money in a variety of other ways – by helping them make their content easier to find; by providing advertising tools like AdWords and AdSense; and by providing other platforms to sell and make their works available, like Google eBooks.

Google has also been an industry leader in developing innovative measures to protect copyright and help rightsholders control their content online. For example, Google has dedicated more than 50,000 engineering hours and more than \$30 million to develop Content ID, our cutting-edge copyright protection tool that helps rightsholders control their content and make money on YouTube. This powerful technology scans the more than 48 hours of video uploaded to YouTube every minute and, within seconds, compares it against more than six million reference files provided by participating rightsholders. Content ID has proven to be an enormous success and is being used by a long list of content owners worldwide to make their own choices about how, where, when, or whether they want their content to appear on YouTube. Content ID is a win-win solution for YouTube and content owners alike: more than one-third of all revenues generated on YouTube are the result of monetization decisions made possible by Content ID.

The DMCA notice-and-takedown process continues to be a cornerstone of our content protection efforts. During 2010, we processed DMCA takedown notices for approximately three million items across all of our products. Already in 2011 we have processed takedown notices for nearly five million items, and we have done so more quickly and efficiently than ever before.

Last December, we announced that we were building new tools and procedures to enable us to act on reliable DMCA takedown requests within 24 hours. We are happy to report that we have met and exceeded that goal. For Web Search, more than 75 percent of DMCA takedown notices are coming in using our new tools, and our average turnaround time for those notices is now less than six hours. On Blogger, we are testing tools that enable nearly instantaneous removals for trusted content partners.

We also employ a wide array of procedures and expend considerable financial resources to prevent our advertising products from being used to monetize material that infringe copyright. For example, our AdSense program enables website publishers to display ads alongside their content. Our policies prohibit the use of this program for infringing sites, and we use automated and manual review to weed out abuse. In 2010, we took action on our own initiative against nearly 12,000 sites for violating this policy. Already in 2011, we have taken action against 12,000 more. We also respond swiftly when notified by

rightsholders, and we recently agreed to improve our AdSense anti-piracy review procedures and are working together with rightsholders on better ways to identify websites that violate our policies.

We are also helping to lead industry-wide solutions through our work with the Interactive Advertising Bureau (“IAB”), comprised of more than 460 leading media and technology companies. The IAB has established quality-assurance guidelines through which participating advertising companies will take standardized steps to enhance buyer control over the placement and context of advertising and build brand safety. Google was among the first companies to certify our compliance with these guidelines.

Google also expends great effort to meet the challenge of counterfeit goods. Since June 2010, we have shut down nearly 150,000 accounts for attempting to use sponsored links to advertise counterfeit goods. Most of these were proactive removals, done on our own initiative—we received legitimate complaints about less than one quarter of one per cent of our advertisers. Even more ads were blocked on suspicion of policy violations. Our automated tools analyze thousands of signals to help prevent bad ads from being shown in sponsored links. Last year alone we invested \$60 million in efforts to prevent violations of our ad policies.

Nevertheless, despite the best efforts of the online advertising industry, more can be done. Some publishers deliberately take steps to evade detection systems, meaning some bad sites will inevitably slip through. Technologically sophisticated players use tactics like “cloaking” (showing one version of their site to the public and a different version to Google) to evade the protections that Google and other companies put in place. We will need the cooperation of rightsholders to identify and terminate our services to the sites that manage to evade our procedures. While the industry is aggressively going after this abuse, it is a cat-and-mouse game to stay ahead of the bad actors. Google is committed to being an industry leader in eradicating this behavior.

### ***Principles for a Consensus Solution***

As we work together to develop appropriately targeted measures to counter foreign rogue sites, we urge you to consider the six principles that Google’s General Counsel, Kent Walker, offered before this Committee seven months ago:

- (1) Policymakers should aim squarely at the “worst of the worst” foreign websites without ensnaring legitimate technologies and businesses. At a minimum, this means tailoring the definitions to capture only sites that are violating the law and operating outside the DMCA safe harbors.
- (2) New legislation should not alter common law secondary liability principles or undermine the DMCA.
- (3) The DMCA strikes the right balance for search engines.
- (4) Legislation should not interfere with the health and stability of the Internet, particularly with regard to the DNS.
- (5) Policymakers should foreclose private rights of action and tailor intermediary requirements appropriately.
- (6) Policymakers should dismantle barriers to encourage greater proliferation of compelling, legal offerings for copyrighted works online.

Reiterating the statements of Kent Walker before this Committee, we believe that an approach that focuses on advertising and payment services (both of which Google offers) is the most promising path toward an effective solution. So long as there is money to be made by rogue sites offering pirated content and counterfeit goods, efforts to make sites “disappear” from the Internet will be fruitless. Just like a hydra, every effort to behead one site will likely give rise to multiple new rogue sites.

By creating new remedies focused on removing the financial incentive for foreign rogue sites, this Committee can make a valuable contribution to the battle against piracy and counterfeiting. However, these remedies should be reserved for foreign sites that operate beyond the reach of U.S. courts, should not undermine the DMCA safe harbors for other activities, and should be administered by courts in order to preserve the due process rights of those accused. We look forward to working with members of the Committee on legislative language that would develop this alternative approach.

### **Conclusion**

In sum, Google has grave concerns about SOPA in its current form, and we are not alone. The technology community, venture capitalists, academia, human rights groups, computer security experts, and others have all expressed their concerns. We trust that the Committee will take these concerns to heart, and we stand ready to work with you to find solutions, including legislation which can successfully protect intellectual property while safeguarding the legitimate activities online that are fueling economic growth and free expression around the world. Thank you.

**Attachment: Internet Companies Letter on SOPA**

November 15, 2011

The Honorable Pat Leahy  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

The Honorable Chuck Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

The Honorable Lamar Smith  
Chairman  
Committee on the Judiciary  
House of Representatives  
Washington, DC 20515

The Honorable John Conyers, Jr.  
Ranking Member  
Committee on the Judiciary  
House of Representatives  
Washington, DC 20515

Dear Chairman Leahy, Ranking Member Grassley, Chairman Smith and Ranking Member Conyers:

The undersigned Internet and technology companies write to express our concern with legislative measures that have been introduced in the United States Senate and United States House of Representatives, S. 968 (the "PROTECT IP Act") and H.R. 3261 (the "Stop Online Piracy Act").

We support the bills' stated goals -- providing additional enforcement tools to combat foreign "rogue" websites that are dedicated to copyright infringement or counterfeiting. Unfortunately, the bills as drafted would expose law-abiding U.S. Internet and technology companies to new uncertain liabilities, private rights of action, and technology mandates that would require monitoring of web sites. We are concerned that these measures pose a serious risk to our industry's continued track record of innovation and job creation, as well as to our Nation's cybersecurity. We cannot support these bills as written and ask that you consider more targeted ways to combat foreign "rogue" websites dedicated to copyright infringement and trademark counterfeiting, while preserving the innovation and dynamism that has made the Internet such an important driver of economic growth and job creation.

One issue merits special attention. We are very concerned that the bills as written would seriously undermine the effective mechanism Congress enacted in the Digital Millennium Copyright Act (DMCA) to

provide a safe harbor for Internet companies that act in good faith to remove infringing content from their sites. Since their enactment in 1998, the DMCA's safe harbor provisions for online service providers have been a cornerstone of the U.S. Internet and technology industry's growth and success. While we work together to find additional ways to target foreign "rogue" sites, we should not jeopardize a foundational structure that has worked for content owners and Internet companies alike and provides certainty to innovators with new ideas for how people create, find, discuss, and share information lawfully online.

We are proud to be part of an industry that has been crucial to U.S. economic growth and job creation. A recent McKinsey Global Institute report found that the Internet accounts for 3.4 percent of GDP in the 13 countries that McKinsey studied, and, in the U.S., the Internet's contribution to GDP is even larger. If Internet consumption and expenditure were a sector, its contribution to GDP would be greater than energy, agriculture, communication, mining, or utilities. In addition, the Internet industry has increased productivity for small and medium-sized businesses by 10%. We urge you not to risk either this success or the tremendous benefits the Internet has brought to hundreds of millions of Americans and people around the world.

We stand ready to work with the Congress to develop targeted solutions to address the problem of foreign "rogue" websites.

Thank you in advance for your consideration.

AOL Inc.  
eBay Inc.  
Facebook Inc.  
Google Inc.  
LinkedIn Corporation  
Mozilla Corp.  
Twitter, Inc.  
Yahoo! Inc.  
Zynga Game Network

