December 22, 2014

Jim Hood
Mississippi Attorney General
Walter Sillers Building
550 High Street, Suite 1200
Jackson, MS 39201

Dear Attorney General Hood:

According to recent news reports, your office, in active coordination with the Motion Picture Association of America (MPAA) and its member companies, has been and remains engaged in a coordinated campaign to shut down and block access to individual websites through backdoor methods resoundingly rejected by the public and federal lawmakers.

Publications including the *New York Times*, the *Huffington Post*, and *The Verge* are reporting that the MPAA responded to the failure of the Stop Online Piracy Act (SOPA) in 2012 by quietly searching for alternate means to accomplish key provisions of the bill, such as website blocking and search filtering. It is our understanding that those efforts include developing legal theories and even drafting civil investigation demand letters for state attorneys general to facilitate actions against websites and search engines. The goal of these efforts mirrors the goal of SOPA: to create new legal tools that will compel online service providers to remove content from the Internet with little, if any, meaningful due process.

While we recognize these reports may be incomplete, the available information nevertheless leaves us deeply concerned. As demonstrated in the debate over SOPA, compelled website blocking by online service providers poses an unjustifiable threat to the security of the Domain Name System (DNS), the basic address book of the Internet. Similarly, requiring third parties to filter the contents of DNS lookups and search results threatens the Internet as a tool and forum for free expression.

Despite these risks, you told the *Huffington Post* you agreed with the methods of the ill-fated SOPA legislation. We beg to differ, as do the engineers who created the Internet, the organizations and businesses that depend upon a secure and robust Internet infrastructure, and the legions of Internet users who spoke out against SOPA in 2011 and 2012. When Congress tried to pass SOPA in 2011-2012, millions of Americans signed petitions, called and emailed their Congressional representatives, and commented on social media platforms, all firmly opposing attempts to limit online speech by blocking websites without appropriate legal process. SOPA was a bad idea at the federal level, and any SOPA revival on a state level is an equally bad idea that, we are confident, will be equally unacceptable to the public.

We have included several letters highlighting the original opposition to SOPA to remind you of the depth of the problems with this approach and the principled opposition to curtailing free speech that it first provoked.

Sincerely,

American Library Association
Center for Democracy and Technology
Computer and Communications Industry Association
Consumer Electronics Association
Demand Progress
Electronic Frontier Foundation
Engine Advocacy
Free Press
FreedomWorks
New America's Open Technology Institute
Public Knowledge
R StreetRootstrikers

Public Interest Groups Letter

November 15, 2011

The Honorable Lamar Smith Chairman
Committee on the Judiciary
2138 Rayburn House Office Building Washington, DC 20515

The Honorable John Conyers, Jr. Ranking Member
Committee on the Judiciary
2138 Rayburn House Office Building Washington, DC 20515

Re: H.R. 3261, the Stop Online Piracy Act

Dear Chairman Smith and Ranking Member Conyers,

The undersigned advocates and organizations write to express our deep concern with H.R. 3261, the "Stop Online Piracy Act" (SOPA). While we support appropriate copyright enforcement and want to ensure that creators around the world have the opportunity to be compensated for their works, SOPA as constructed would come at too high a cost to Internet communication and noninfringing online expression. The bill would set an irreversible precedent that encourages the fracturing of the Internet, undermines freedom of expression worldwide, and has numerous other unintended and harmful consequences.

We do not dispute that there are hubs of online infringement. But the definitions of the sites that would be subject to SOPA's remedies are so broad that they would encompass far more than those bad actors profiting from infringement. By including all sites that may – even inadvertently – "facilitate" infringement, the bill raises serious concerns about overbreadth. Under section 102 of the bill, a nondomestic startup video-sharing site with thousands of innocent users sharing their own noninfringing videos, but a small minority who use the site to criminally infringe, could find its domain blocked by U.S. DNS operators. Countless non-infringing videos from the likes of aspiring artists, proud parents, citizen journalists, and human rights activists would be unduly swept up by such an action. Furthermore, overreach resulting from bill is more likely to impact the operators of smaller websites and services that do not have the legal capacity to fight false claims of infringement.

Relying on an even broader definition of "site dedicated to theft of US property," section 103 of SOPA creates a private right of action of breathtaking scope. Any rightsholder could cut off the financial lifeblood of services such as search engines, user-generated content platforms, social media, and cloud-based storage unless those services actively monitor and police user activity to the rightsholder's satisfaction. A mere accusation by any rightsholder would be sufficient to require payment systems and ad networks to terminate doing business with the service; the accused service's only recourse would be to send a counter-notice, at which point it would be at the networks' discretion whether to reinstate the service's access to payments and advertising. This would bypass and effectively overturn the basic framework of the Digital Millennium Copyright Act (DMCA), by pushing user-driven sites like Twitter, YouTube, and Facebook to implement ever-more elaborate monitoring systems to "confirm," to the satisfaction of the most aggressive and litigious rightsholder, whether individual users are exchanging infringing content. These and other sites have flourished under the DMCA safe harbor, which provides certainty concerning the legal responsibilities of online service providers and expressly rejects a de facto legal obligation to actively track and police user

behavior. Creating such an obligation would be hugely damaging to Internet innovation, particularly for smaller, emerging sites and individuals. It would also carry major consequences for users' legitimate privacy interests.

We also have serious concerns about the inclusion the provisions in section 102 to require ISPs to filter Domain Name System (DNS) requests or otherwise try to "prevent access" to targeted websites.[1] DNS-filtering is trivial to circumvent and will be ineffective at stopping infringement. Where it does have an impact, that effect is likely to be overbroad, sweeping in legitimate online content. We have witnessed this already in the case of mooo.com, the seizure of which led to upwards of 84,000 innocent subdomains being blocked.[2]

In addition, mandated filtering would undermine the U.S. government's commitment to advancing a single, global Internet. Its inclusion risks setting a precedent for other countries, even democratic ones, to use the same mechanisms to enforce a range of domestic policies, effectively balkanizing the global medium of the Internet. Simply declaring that filtering aimed at copyright and trademark infringement is different from filtering with more sinister motives does not change the message this would send to the world – that the United States is legitimizing methods of online censorship to enforce its domestic laws. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association.

DNS-filtering also raises very real cybersecurity concerns.[3] It conflicts with Secure DNS (DNSSEC), and circumventing the filters will risk making domestic networks and users more vulnerable to cybersecurity attacks and identity theft as users migrate to offshore DNS providers not subject to filtering orders. Given the ease with which DNS filters can be circumvented, there is strong reason to doubt that its benefits are worth these costs.

The undersigned organizations recognize the importance of addressing truly illicit behavior online. We share the overall goals of many of SOPA's supporters – preventing large-scale commercial infringement and ensuring that creativity and expression thrive. Intellectual property infringement breaks the law online or off, but SOPA is not the right way to stop it. Current enforcement mechanisms were designed to avoid the countervailing harms of conscripting intermediaries into being points of control on the Internet and deciding what is and what is not copyright-infringing expression. As drafted, SOPA radically alters digital copyright policy in ways that will be detrimental to online expression, innovation, and security.

Sincerely,

American Library Association
Association of Research Libraries
Center for Democracy & Technology
Competitive Enterprise Institute
Demand Progress
Electronic Frontier Foundation Freedom House
Human Rights First
Human Rights Watch Internews
New America Foundation's Open Technology Initiative
Public Knowledge
TechFreedom

[1] These concerns also apply to the DNS Filtering provisions included S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, also known as the PROTECT IP Act, which

[2] *See* Thomas Claburn, *ICE Confirms Inadvertent Web Site Seizures, Information Week*, February 18, 2011. http://www.informationweek.com/news/security/vulnerabilities/229218959?cid=RSSfeed_IWK_All.

[3] *See* Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, and Paul Vixie, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, May 2011 http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Internet Engineers Letter, December 15, 2011

We, the undersigned, have played various parts in building a network called the Internet. We wrote and debugged the software; we defined the standards and protocols that talk over that network. Many of us invented parts of it. We're just a little proud of the social and economic benefits that our project, the Internet, has brought with it.

Last year, many of us wrote to you and your colleagues to warn about the proposed "COICA" copyright and censorship legislation. Today, we are writing again to reiterate our concerns about the SOPA and PIPA derivatives of last year's bill, that are under consideration in the House and Senate. In many respects, these proposals are worse than the one we were alarmed to read last year.

If enacted, either of these bills will create an environment of tremendous fear and uncertainty for technological innovation, and seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure. Regardless of recent amendments to SOPA, both bills will risk fragmenting the Internet's global domain name system (DNS) and have other capricious technical consequences. In exchange for this, such legislation would engender censorship that will simultaneously be circumvented by deliberate infringers while hampering innocent parties' right and ability to communicate and express themselves online.

All censorship schemes impact speech beyond the category they were intended to restrict, but these bills are particularly egregious in that regard because they cause entire domains to vanish from the Web, not just infringing pages or files. Worse, an incredible range of useful, law-abiding sites can be blacklisted under these proposals. In fact, it seems that this has already begun to happen under the nascent DHS/ICE seizures program.

Censorship of Internet infrastructure will inevitably cause network errors and security problems. This is true in China, Iran and other countries that censor the network today; it will be just as true of American censorship. It is also true regardless of whether censorship is implemented via the DNS, proxies, firewalls, or any other method. Types of network errors and insecurity that we wrestle with today will become more widespread, and will affect sites other than those blacklisted by the American government.

The current bills -- SOPA explicitly and PIPA implicitly -- also threaten engineers who build Internet systems or offer services that are not readily and automatically compliant with censorship actions by the U.S. government. When we designed the Internet the first time, our priorities were reliability, robustness and minimizing central points of failure or control. We are alarmed that Congress is so close to mandating censorship-compliance as a design requirement for new Internet innovations. This can only damage the security of the network, and give authoritarian governments more power over what their citizens can read and publish.

The US government has regularly claimed that it supports a free and open Internet, both domestically and abroad. We cannot have a free and open Internet unless its naming and routing systems sit above the political concerns and objectives of any one government or industry. To date, the leading role the US has played in this infrastructure has been fairly uncontroversial because America is seen as a trustworthy arbiter and a neutral bastion of free expression. If the US begins to use its central position in the network for censorship that advances its political and economic agenda, the consequences will be far-reaching and destructive.

Senators, Congressmen, we believe the Internet is too important and too valuable to be endangered in this way, and implore you to put these bills aside.

Signed,

- **Vint Cerf**, co-designer of TCP/IP, one of the "fathers of the Internet", signing as private citizen
- **Paul Vixie,** author of BIND, the most widely-used DNS server software, and President of the Internet Systems Consortium
- **Tony Li**, co-author of BGP (the protocol used to arrange Internet routing); chair of the IRTF's Routing Research Group; a Cisco Fellow; and architect for many of the systems that have actually been used to build the Internet
- **Steven Bellovin**, invented the DNS cache contamination attack; co-authored the first book on Internet security; recipient of the 2007 NIST/NSA National Computer Systems Security Award and member of the DHS Science and Technology Advisory Committee
- **Jim Gettys**, editor of the HTTP/1.1 protocol standards, which we use to do everything on the Web
- **Dave Kristol**, co-author, RFCs 2109, 2965 (Web cookies); contributor, RFC 2616 (HTTP/1.1)
- **Steve Deering, Ph.D.**, invented the IP multicast feature of the Internet; lead designer of IPv6 (version 6 of the Internet Protocol)
- **David Ulevitch**, David Ulevitch, CEO of OpenDNS, which offers alternative DNS services for enhanced security.
- **Elizabeth Feinler**, director of the Network Information Center (NIC) at SRI International, administered the Internet Name Space from 1970 until 1989 and developed the naming conventions for the internet top level domains (TLDs) of .mil, .gov, .com, .org, etc. under contracts to DoD
- **Robert W. Taylor**, founded and funded the beginning of the ARPAnet; founded and managed the Xerox PARC Computer Science Lab which designed and built the first networked personal computer (Alto), the Ethernet, the first internet protocol and internet, and desktop publishing
- **Fred Baker**, former IETF chair, has written about 50 RFCs and contributed to about 150 more, regarding widely used Internet technology
- **Dan Kaminsky**, Chief Scientist, DKH
- **Esther Dyson**, EDventure; founding chairman, ICANN; former chairman, EFF; active investor in many start-ups that support commerce, news and advertising on the Internet; director, Sunlight Foundation
- **Walt Daniels,** IBM’s contributor to MIME, the mechanism used to add attachments to emails
- **Nathaniel Borenstein**, Chief Scientist, Mimecast; one of the two authors of the MIME protocol, and has worked on many other software systems and protocols, mostly related to e-mail and payments
- **Simon Higgs**, designed the role of the stealth DNS server that protects a.root-servers.net; worked on all versions of Draft Postel for creating new TLDs and addressed trademark issues with a complimentary Internet Draft; ran the shared-TLD mailing list back in 1995 which defined the domain name registry/registrar relationship; was a root server operator for the Open Root Server Consortium; founded coupons.com in 1994
- **John Bartas**, was the technical lead on the first commercial IP/TCP software for IBM PCs in 1985-1987 at The Wollongong Group. As part of that work, developed the first tunneling RFC, rfc-1088
- **Nathan Eisenberg**, Atlas Networks Senior System Administrator; manager of 25K sq. ft. of data centers which provide services to Starbucks, Oracle, and local state
- **Dave Crocker**, author of Internet standards including email, DKIM anti-abuse, electronic data interchange and facsimile, developer of CSNet and MCI national email services, former IETF Area Director for network management, DNS and standards, recipient of IEEE Internet Award for contributions to email, and serial entrepreneur

- **Craig Partridge,** architect of how email is routed through the Internet; designed the world's fastest router in the mid 1990s
- **Doug Moeller**, Chief Technology Officer at Autonet Mobile
- **John Todd**, Lead Designer/Maintainer - Freenum Project (DNS-based, free telephony/chat pointer system), http://freenum.org/
- **Alia Atlas**, designed software in a core router (Avici) and has various RFCs around resiliency, MPLS, and ICMP
- **Kelly Kane**, shared web hosting network operator
- **Robert Rodgers**, distinguished engineer, Juniper Networks, signing as a private citizen
- **Anthony Lauck**, helped design and standardize routing protocols and local area network protocols and served on the Internet Architecture Board
- **Ramaswamy Aditya**, built various networks and web/mail content and application hosting providers including AS10368 (DNAI) which is now part of AS6079 (RCN); did network engineering and peering for that provider; did network engineering for AS25 (UC Berkeley); currently does network engineering for AS177-179 and others (UMich)
- **Blake Pfankuch**, Connecting Point of Greeley, Network Engineer
- **Jon Loeliger**, has implemented OSPF, one of the main routing protocols used to determine IP packet delivery; at other companies, has helped design and build the actual computers used to implement core routers or storage delivery systems; at another company, installed network services (T-1 lines and ISP service) into Hotels and Airports across the country
- **Jim Deleskie,** internetMCI Sr. Network Engineer, Teleglobe Principal Network Architect
- **David Barrett**, Founder and CEO, Expensify
- **Mikki Barry**, VP Engineering of InterCon Systems Corp., creators of the first commercial applications software for the Macintosh platform and the first commercial Internet Service Provider in Japan
- **Peter Rubenstein**,helped to design and build the AOL backbone network, ATDN.
- **David Farber**, distinguished Professor CMU; Principal in development of CSNET, NSFNET, NREN, GIGABIT TESTBED, and the first operational distributed computer system; EFF board member
- **Bradford Chatterjee**, Network Engineer, helped design and operate the backbone network for a nationwide ISP serving about 450,000 users
- **Gary E. Miller** Network Engineer specializing in eCommerce
- **Jon Callas**, worked on a number of Internet security standards including OpenPGP, ZRTP, DKIM, Signed Syslog, SPKI, and others; also participated in other standards for applications and network routing
- **John Kemp**, Principal Software Architect, Nokia; helped build the distributed authorization protocol OAuth and its predecessors; former member of the W3C Technical Architecture Group
- **Christian Huitema**, worked on building the Internet in France and Europe in the 80's, and authored many Internet standards related to IPv6, RTP, and SIP; a former member of the Internet Architecture Board
- **Steve Goldstein**, Program Officer for International Networking Coordination at the National Science Foundation 1989-2003, initiated several projects that spread Internet and advanced Internet capabilities globally
- **David Newman**, 20 years' experience in performance testing of Internet
- infrastructure; author of three RFCs on measurement techniques (two on firewall performance, one on test traffic contents)
- **Justin Krejci**, helped build and run the two biggest and most successful municipal wifi networks located in Minneapolis, MN and Riverside, CA; building and running a new FTTH network in Minneapolis
- **Christopher Liljenstolpe**, was the chief architect for AS3561 (at the time about 30% of the Internet backbone by traffic), and AS1221 (Australia's main Internet infrastructure)
- **Joe Hamelin**, co-founder of Seattle Internet Exchange (http://www.seattleix.net) in 1997, and former peering engineer for Amazon in 2001
- **John Adams**, operations engineer at Twitter, signing as a private citizen
- **David M. Miller**, CTO / Exec VP for DNS Made Easy (IP Anycast Managed Enterprise DNS provider)
- **Seth Breidbart**, helped build the Pluribus IMP/TIP for the ARPANET
- **Timothy McGinnis**, co-chair of the African Network Information Center Policy Development Working Group, and active in various IETF Working Groups
- **Richard Kulawiec,** 30 years designing/operating academic/commercial/ISP systems and networks
- **Larry Stewart**, built the Etherphone at Xerox, the first telephone system working over a local area network; designed early e-commerce systems for the Internet at Open Market
- **John Pettitt**, Internet commerce pioneer, online since 1983, CEO Free Range Content Inc.; founder/CTO CyberSource & Beyond.com; created online fraud protection software that processes over 2 billion transaction a year
- **Brandon Ross**, Chief Network Architect and CEO of Network Utility Force LLC
- **Chris Boyd**, runs a green hosting company and supports EFF-Austin as a board member

- **Dr. Richard Clayton,** designer of Turnpike, widely used Windows-based Internet access suite; prominent Computer Security researcher at Cambridge University
- **Robert Bonomi**, designed, built, and implemented, the Internet presence for a number of large corporations
- **Owen DeLong**, member of the ARIN Advisory Council who has spent more than a decade developing better IP addressing policies for the internet in North America and around the world
- **Baudouin Schombe**, blog design and content trainer
- **Lyndon Nerenberg**, Creator of IMAP Binary extension (RFC 3516)
- **John Gilmore,** co-designed BOOTP (RFC 951), which became DHCP, the way you get an IP address when you plug into an Ethernet or get on a WiFi access point; current EFF board member
- **John Bond**, Systems Engineer at RIPE NCC maintaining AS25152 (k.root-servers.net.) and AS197000 (f.in-addr-servers.arpa. ,f.ip6-servers.arpa.); signing as a private citizen
- **Stephen Farrell**, co-author on about 15 RFCs
- **Samuel Moats**, senior systems engineer for the Department of Defense; helps build and defend the networks that deliver data to Defense Department users
- **John Vittal**, created the first full email client and the email standards still in use today
- **Ryan Rawdon**, built out and maintains the network infrastructure for a rapidly growing company in our country's bustling advertising industry; was on the technical operations team for one of our country's largest residential ISPs
- **Brian Haberman**, has been involved in the design of IPv6, IGMP/MLD, and NTP within the IETF for nearly 15 years
- **Eric Tykwinski**, Network Engineer working for a small ISP based in the Philadelphia region; currently maintains the network as well as the DNS and server infrastructure
- **Noel Chiappa**, has been working on the lowest level stuff (the IP protocol level) since 1977; name on the 'Birth of the Internet' plaque at Stanford); actively helping to develop new 'plumbing' at that level
- **Robert M. Hinden**, worked on the gateways in the early Internet, author of many of the core IPv6 specifications, active in the IETF since the first IETF meeting, author of 37 RFCs, and current Internet Society Board of Trustee member
- **Alexander McKenzie**, former member of the Network Working Group and participated in the design of the first ARPAnet Host protocols; was the manager of the ARPAnet Network Operation Center that kept the network running in the early 1970s; was a charter member of the International Network Working Group that developed the ideas used in TCP and IP
- **Keith Moore**, was on the Internet Engineering Steering Group from 1996-2000, as one of two Area Directors for applications; wrote or co-wrote technical specification RFCs associated with email, WWW, and IPv6 transition
- **Guy Almes**, led the connection of universities in Texas to the NSFnet during the late 1980s; served as Chief Engineer of Internet2 in the late 1990s
- **David Mercer**, formerly of The River Internet, provided service to more of Arizona than any local or national ISP
- **Paul Timmins**, designed and runs the multi-state network of a medium sized telephone and internet company in the Midwest
- **Stephen L. Casner**, led the working group that designed the Real-time Transport Protocol that carries the voice signals in VoIP systems
- **Tim Rutherford,** DNS and network administrator at C4
- **Mike Alexander**, helped implement (on the Michigan Terminal System at the University of Michigan) one of the first EMail systems to be connected to the Internet (and to its predecessors such as Bitnet, Mailnet, and UUCP); helped with the basic work to connect MTS to the Internet; implemented various IP related drivers on early Macintosh systems: one allowed TCP/IP connections over ISDN lines and another made a TCP connection look like a serial port
- **John Klensin, Ph.D.**, early and ongoing role in the design of Internet applications and coordination and administrative policies; former IAB Chair and former AT&T Internet Architecture VP
- **L. Jean Camp,** former Senior Member of the Technical Staff at Sandia National Laboratories, focusing on computer security; eight years at Harvard's Kennedy School; tenured Professor at Indiana Unviersity's School of Informatics with research addressing security in society.
- **Louis Pouzin**, designed and implemented the first computer network using datagrams (CYCLADES), from which TCP/IP was derived
- **Carl Page**, helped found eGroups, the biggest social network
- of its day, 14 million users at the point of sale to Yahoo for around $430,000,000, at which point it became Yahoo Groups
- **Phil Lapsley**, co-author of the Internet Network News Transfer Protocol (NNTP), RFC 977, and developer of the NNTP reference implementation

- **Jack Haverty (MSEE, BSEE MIT 1970)**, Principal Investigator for several DARPA projects including the first Internet development and operation; Corporate Network Architect for BBN; Founding member of the IAB/ICCB; Internet Architect and Corporate Founding Member of W3C for Oracle Corporation
- **Glenn Ricart**, Managed the original (FIX) Internet interconnection point
- **Ben Laurie**, Apache Software Foundation founder, OpenSSL core team member, security researcher. Over half the secure websites on the Internet are powered by his software.
- **Chris Wellens** President & CEO InterWorking Labs
- **Chris Morrow** Network Security Engineer at Google, and previously at UUNET. Involved in several IETF routing and security working groups.
- **Dave Shambley**, entrepreneur and IEEE member
- **Bill Jennings**, who was VP of Engineering at Cisco for 10 years and responsible for building much of the hardware and embedded software for Cisco's core router products and high-end Ethernet switches
- **Bernie Cosell** coauthored the original IMP code, Terminal-IMP [TIP] and monitoring code for the NOC.
- **Leonard Kleinrock**, one of the "fathers of the Internet", created the mathematical theory of packet networks, ran the UCLA lab that served as the first node of the ARPANET, and supervised the transmission of its first message.
- **Rebecca Hargrave Malamud**, helped advance many large-scale Internet projects, and have been working the web since its invention.

Entrepreneur's Letter, December 9, 2011

To Members of the United States Congress:

The undersigned are 160 entrepreneurs, founders, CEOs and executives who have been involved in 349 technology start-ups, and who have created over 65,000 jobs directly through our companies and hundreds of thousands, if not millions, more through the technologies we invented, funded, brought to market and made mainstream. We write today urging you to reject S.968, the PROTECT IP Act, also known as "PIPA." We appreciate the stated purpose of the bill, but we fear that if PIPA is allowed to become law in its present form, it will hurt economic growth and chill innovation in legitimate services that help people create, communicate, and make money online.

It is a truism that small businesses create significant economic growth and jobs, but it is more accurate to say that new businesses, including tech start-ups, are most important.[1] The Internet is a key engine of today's economy,[2] and much of its economic contribution is attributable to companies that did not even exist 10 or even 5 years ago. The Internet has also created new opportunities for artists and other content creators -- today, there is more content being created by more people on more platforms (including some of our businesses) than ever before.

We are not opposed to copyright or the bill's intent, but we do not think this bill will actually fulfill copyright's purpose of encouraging innovation and creativity. While the bill will create uncertainty for many legitimate businesses and in turn undermine innovation and creativity on those services, the dedicated pirates who use and operate "rogue" sites will simply migrate to platforms that conceal their activities.

Our concerns include the following:

- The notion of sites "dedicated to infringing activities" is vague and ripe for abuse, particularly when combined with a private right of action for rightsholders: Legitimate sites with legitimate uses can also in many cases be used for piracy. Historically, overzealous rightsholders have tried to stop many legitimate technologies that disrupted their existing business models and facilitated some unauthorized activity. The following technologies were condemned at one point or another - the gramophone (record player), the player piano, radio, television, the photocopier, cable TV, the VCR, the DVR, the mp3 player and video hosting platforms. Even though these technologies obviously survived, many individual businesses like DVR-maker ReplayTV and video platform Veoh were not so fortunate - those companies went bankrupt due to litigation costs, and sold their remaining assets to foreign companies.

PIPA provides a new weapon against legitimate businesses and "rogue" sites alike, and the concern in this context is not merely historical or theoretical. Recent press reports noted that advertising giant WPP's GroupM subsidiary had put together a list of 2,000 sites that were

declared to be “supporting piracy,” on which none of its advertising would be allowed to appear. That list - which was put together with suggestions from GroupM clients - includes Vibe.com, the online version of the famed Vibe Magazine, founded by Quincy Jones, and a leading publication for the hip hop and R&B community. It also included the Internet Archive’s Wayback Machine, which preserves copies of Web pages in order to fill a similar function as libraries.

When a famous magazine and a library get lumped in with “rogue pirate sites” in this way, it’s not hard to see how an overzealous copyright holder might seek to shut legitimate businesses down through PIPA.

- The bill would create significant burdens for smaller tech companies: One of the key reasons why startups and innovative small businesses became the success stories we know of today was protection from misguided lawsuits under the safe harbors of Section 512 of the Digital Millennium Copyright Act (DMCA). By properly putting the legal liability on the actual actors of infringement rather than third-parties, Congress wisely ensured that service providers, such as many of the companies represented in this letter, could flourish.

PIPA would put new burdens and possible liability on independent third parties, including payment processors, advertising firms, information location tools and others. The definitions here are incredibly vague, and many companies signed below could fall under the broad definitions of “information location tools,” meaning costly changes to their infrastructure, including how we remain in compliance with blocking orders on an ever-changing Internet. Separately, including a private right of action means that any rightsholder can tie up a service provider in costly legal action, even if it eventually turns out to not be valid. Given the broad definitions used above for sites “supporting piracy,” 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.

These burdens will be particularly intense for small businesses who can’t easily afford the legal fees, infrastructure costs or staff required to remain in compliance with broadly worded laws in a rapidly changing ecosystem.

Legitimate services already do their part by following the notice-and-takedown system of the DMCA. While we take these types of legal responsibilities seriously and already take on costs to do so, that’s no reason to pile on additional regulations.

- Breaking DNS will harm our ability to build new, safe, and secure services. As detailed in a recent whitepaper by some of the foremost experts in Internet architecture and security, PIPA will fragment parts of key Internet infrastructure, and disrupt key security tools in use today.[3] Interfering in the basic technological underpinnings of the Internet that we all rely on today would be a huge anchor on innovation in many of our companies.

As Web entrepreneurs and Web users, we want to ensure that artists and great creative content can thrive online. But this isn't the right way to address the underlying issue. Introducing this new regulatory weapon into the piracy arms race won't stop the arms race, but it will ensure there will be more collateral damage along the way. There are certainly challenges to succeeding as a content creator online, but the opportunities are far greater than the challenges, and the best way to address the latter is to create more of the former.

In other words, innovation in the form of more content tools, platforms and services is the right way to address piracy -- while also creating new jobs and fueling economic growth. Entrepreneurs like us can help do that; PIPA can't.

Sincerely,
(In alphabetical order by name, followed by companies either founded or where one was in a job-creating executive role)

Jonathan Abrams
Nuzzel, Founders Den, Socializr, Friendster, HotLinks

Asheesh Advani
Covestor, Virgin Money USA, CircleLending

David Albert
Hackruiter

Will Aldrich
SurveyMonkey, TripIt, Yahoo

Courtland Allen
Syphir, Tyrant

Lloyd Armbrust
OwnLocal.com

Jean Aw
NOTCOT Inc.

Joshua Baer
Capital Factory, OtherInbox, UnsubCentral, SKYLIST

Andy Baio
Upcoming, Kickstarter

Edward Baker
Friend.ly

David Barrett
Expensify

Jonathan Baudanza
beatlab.com, Rupture

Katia Beauchamp
Birchbox

Idan Beck
Incident Technologies

Justin Beck
PerBlue

Matthew Bellows
Yesware Inc., WGR Media

David Berger
XL Marketing, Caridian Marketing Labs

Nicholas Bergson-Shilcock
Hackruiter

Ted Blackman
Course Zero Automation, Motion Arcade

Matthew Blumberg
MovieFone, ReturnPath

Nic Borg
Edmodo

Bruce Bower
Plastic Jungle, Blackhawk Network, Reactrix, Soliloquy Learning, ZapMe! Corporation, YES! Entertainment

Josh Buckley
MinoMonsters

John Buckman
Lyris, Magnatune, BookMooch

Justin Cannon
Lingt Language, EveryArt

Teck Chia
OpenAppMkt, Omigosh LLC, Gabbly.com

Bill Clerico
WePay

Michael Clouser
iLoding, Market Diligence, CEO Research, New Era Strategies

Zach Coelius
Triggit, Votes For Students, Coelius Enterprises

John Collison
Stripe

Ben Congleton
Olark, Nethernet

Dave Copps
PureDiscovery, Engenium

Jon Crawford
Storenvy

Dennis Crowley
Foursquare, Dodgeball

Angus Davis
Swipely, Tellme

Eric DeMenthon
PadMapper.com

Steve DeWald
Proper Suit, Data Marketplace, Maggwire

Chad Dickerson
Etsy

Suhail Doshi
Mixpanel

Natalie Downe
Lanyrd Inc.

Nick Ducoff
Infochimps

Derek Dukes
Jetpac, Dipity, Yahoo!

Jennifer Dulski
The Dealmap

Rod Ebrahimi
ReadyForZero, DirectHost

Chas Edwards
Luminate, Digg, Federated Media, MySimon

Dale Emmons
Vidmakr

David Federlein
Fowlsound Productions, Soapbox Coffee, Inc.

Mark Fletcher
ONElist, Bloglines

Andrew Fong
Kirkland North

Tom Frangione
Simply Continuous, Telphia

Brian Frank
Live Colony

Ken Fromm
Vivid Studios, Loomia, Iron.io

Nasser Gaemi
BigDates, ASAM International

Matt Galligan
SimpleGeo, SocialThing

Zachary Garbow
Funeral Innovations

Jud Gardner
Comprehend Systems

David Gibbs
High Speed Access Corp, Darwin Networks, Nomad Innovations

Christopher Golda
BackType

Eyal Goldwerger
TargetSpot, XMPie, WhenU, GoCargo

Jude Gomila
Heyzap

Jeremy Gordon
Department of Behavior and Logic, Secret Level, MagicArts

Steve Greenwood
drop.io

James Gross
Percolate, Federated Media

Sean Grove
Bushido, Inc.

Anupam Gupta
Mixpo

Mike Hagan
LifeShield, Verticalnet, Nutrisystem

Tony Haile
Chartbeat, Chi.mp

Jared Hansen
Breezy

Scott Heiferman
Meetup, Fotolog

Jack Herbeck Jr.
Elroynet, Blu Zone

Eva Ho
Factual, Navigating Cancer, Applied Semantics

Reid Hoffman
LinkedIn, Paypal, Socialnet, Investor in many more, including Facebook, Zynga & GroupOn

Jason Huggins
Blu Zone

Ben Ifeld
Macer Media

Joichi Ito
Neoteny, Digital Garage, Investor in many more including Twitter, Flickr, Kickstarter, Six Apart, Technorati and over 20 other US companies

Jason Jacobs
FitnessKeeper
Daniel James
Three Rings Design

David Jilk
Standing Cloud, eCortex, Xaffire

Noah Kagan
Appsumo, GetGambit

Bill Kallman
Scayl, Varolii

Jon Karl
iovation, ieLogic

Michael Karnjanaprakorn
Skillshare

Bryan Kennedy
Sincerely.com, AppNinjas, Xobni, Pairwise

Derek Kerton
Kerton Group, Telecom Council of Silicon Valley

Drew Kese
Ecount, Orocast

David Kidder
Clickable, SmartRay Network, THINK New Ideas, Net-X

Eric Koger
ModCloth

Kitty Kolding
elicit, House Party, Jupiter

Pete Koomen
Optimizely, CarrotSticks

Brian Krausz
GazeHawk

Amit Kumar
Socialscope

Ryan Lackey
HavenCo, Blue Iraq, Cryptoseal

Jeff Lawson
Twilio, Nine Star, Stubhub, Versity

Peter Lehrman
AxialMarket, Gerson Lehrman Group

Michael Levit
Bluelight.com, Redbooth, Spigot, Founders Den

Michael Lewis
Stellar Semiconductor, Cryptic Studios

Thede Loder
Boxbe, Leverage Information Systems

Marissa Louie
Ness Computing, HeroEX, AD-Village

Eric Marcoullier
OneTrueFan, Gnip, MyBlogLog, IGN

Michael Masnick
Floor64

Jordan Mendelson
SeatMe, Heavy Electrons, SNOCAP, Web Services Inc

Dwight Merriman
DoubleClick, BusinessInsider, Gilt Groupe, 10gen

Scott Milliken
MixRank.com

Michael Montano
BackType

Dave Morgan
Simulmedia, TACODA, Real Media

Zac Morris
Caffeinated Mind Inc.

Rick Morrison
Comprehend Systems

Amy Muller
GetSatisfaction, Rubyred Labs

Darren Nix
Silver Financial

Jeff Nolan
GetSatisfaction, NewsGator, Teqlo, Investor in many more

Craig Ogg
ThisNext, Stamps.com, TrueCar

Alexis Ohanian
Breadpig, Hipmunk, Reddit

Casey Oppenheim
Disconnect, Oppenheim Law

Tim O'Reilly
O'Reilly Media, Safari Books Online, Collabnet, Investor in many more

MIchael Ossareh
Heysan

Gagan Palrecha
Chirply, Zattoo, Sennari

Scott Petry
Authentic8, Postini

Mark Pincus
Zynga, Tribe Networks, SupportSoft, FreeLoader

Chris Poole
4chan, Canvas

Jon Pospischil
PowerSportsStore, AppMentor, FoodTrux, Custora

Jeff Powers
Occipital

Jeff Pulver
140Conf, Pulver.com, Vonage, Free World Dialup, VON Coalition, Vivox

Scott Rafer
Omniar, Lookery, MyBlogLog, Feedster, Fresher, Fotonation, Torque Systems

John Ramey
BuyAds.com, isocket, Maven Ventures, Lythargic Media, electronicfood.com

Vikas Reddy
Occipital

Michael Robertson
DAR.fm, mp3tunes.com, Gizmo5, Linspire, mp3.com

Ian Rogers
TopSpin, MediaCode, FISTFULAYEN, NullSoft/AOL, Yahoo! Music

Avner Ronen
Boxee, Odigo

Zack Rosen
ChapterThree, MissionBicycle, GetPantheon

Oliver Roup
VigLink

Slava Rubin
IndieGoGo

David Rusenko
Weebly

Arram Sabeti
ZeroCater

Peter Schmidt
Midnight Networks, NorthStar Internetworking, Burning Blue Aviation, New England Free Skies Association, Lifting Mind, Analog Devices, Teradyne, Ipanema Technologies, Linear Air

Geoff Schmidt
Tuneprint, MixApp, Honeycomb Guide

Sam Shank
HotelTonight, DealBase, SideStep, TravelPost

Upendra Shardanand
Daylife, The Accelerator Group, Firefly Network

Emmett Shear
Justin.tv

Pete Sheinbaum
LinkSmart, DailyCandy, Alexblake.com, Shop.Eonline.com

Chris Shipley
Guidewire Group

Adi Sideman
Oddcast, Ksolo Karaoke, TargetSpot, YouNow

Chris Sims
Agile Learning Labs

Dan Siroker
Optimizely, CarrotSticks

Rich Skrenta
Blekko, Topix, NewHoo

Bostjan Spetic
Zemanta

Joel Spolsky

StackExchange, Fog Creek Software

Josh Stansfied
Incident Technologies

Mike Tatum
Whiskey Media, Listen.com/Rhapsody, CNET

Brad Templeton
ClariNet Communications, Looking Glass Software, Caller App Inc.

Jack Templin
Lockify, ARC eConsultancy

Craig Tumblison
Bitcove

Khoi Vinh
Lascaux, NYTimes.com, Behavior Design

Joseph Walla
HelloFax

Brian Walsh
Castfire, Three Deep

David Weekly
PBWorks

Jack Welde
Smartling, eMusic, RunTime Technologies, Trio Development

Jeff Widman
PageLever, BrandGlue

Evan Williams
Blogger, Twitter, Obvious

Holmes Wilson
Worcester LLC, Participatory Culture Foundation

Pierre-R Wolff
DataWorks, E-coSearch, AdPassage, Impulse! Buy Network, Kinecta, Impermium, First Virtual Holdings, Revere Data, Tribe Networks

Dennis Yang
Infochimps, Floor64, CNET, mySimon

Chris Yeh
PBWorks, Ustream, Symphoniq

Kevin Zettler
Bushido, Inc.

David Zhao
ZumoDrive

October 31, 2011

Dear Member of Congress:

Last week, Representatives Lamar Smith, Bob Goodlatte, John Conyers, Howard Berman and eight others introduced H.R. 3261, the "Stop Online Piracy Act" ("SOPA"). This legislation has been framed by its sponsors as a vehicle to protect U.S. trademarks and copyrights from foreign "rogue" websites. While we support this concept, H.R. 3261 puts lawful U.S. Internet and technology companies at risk by creating new liabilities, opening the door for vague new technology mandates, imposing significant costs on small businesses, and would create a new unprecedented private right of action regime for intellectual property.

Under this bill, a foreign or domestic Internet site that has broken no U.S. law can nevertheless have its economic lifeblood cut off upon a single notice from a copyright or trademark owner (or perhaps an owner of a patent or trade secret, or possibly even a celebrity with a right of publicity) who alleges that a **single page** of the site "enables or facilitates" illegal activity by third parties.

Moreover, a court can second-guess whether an Internet advertising network is taking all technically feasible and reasonable measures to prevent the placement of ads on a site that has not been found to infringe an existing intellectual property right.

As currently drafted, we believe SOPA is an alarming step backwards in Internet policy creating a thicket of Internet regulations containing 16 new legal definitions for evolving Internet technology (including a definition for the word "including"). Further, the definition of "dedicated to theft of U.S. property" is so broad it would unduly ensnare legitimate companies' websites, products and services.

For example, SOPA would:

- Effectively undermine provisions of the Digital Millennium Copyright Act and Supreme Court jurisprudence that have promoted electronic commerce, cooperation between intellectual property holders and Internet companies, and user privacy. In so doing, SOPA creates a litigation and liability nightmare for Internet and technology companies and social media;
- Create new litigation risks for cloud computing, social networks, and other new technologies that simply have the *potential* of being misused by consumers. Virtually every Internet site that allows user generated content can be subject to suit under SOPA and the bill could force Internet companies to police their users' activities;
- Allow intellectual property owners to seek actions including the termination of advertising and payment services for an entire site even if there is only one page of unlawful content on a site that has millions of pages;

- Institute a regime for Internet censorship by both law enforcement and private actors, undermining the U.S.'s ability to oppose Internet censorship by oppressive, undemocratic countries;
- Allow law enforcement and judges to impose technology mandates on Internet companies to prevent their products and services from being used for illegal conduct by third parties;
- Introduce serious security risks to our communications infrastructure and the critical national infrastructure that depends on it;
- Incentivize ISPs, registrars, registries, ad networks, payment processors, and search engines to take action against a domestic or foreign site when prompted by a rightsholder by providing complete immunity for taking such action while exposing those intermediaries to potential liability if they do not take such action. The property rights of the accused site are tossed away with no recourse and remedy for harm by the website owner;
- Provide for monetary sanctions against intermediaries (payment processors and ad services) in suits initiated by private actors (i.e. private right of action).

In short, this is not a bill that targets "rogue foreign sites." Rather, it allows movie studios, foreign luxury goods manufacturers, patent and copyright trolls, and any holder of any intellectual property right to target lawful U.S. websites and technology companies.

Our industry has and will continue to suggest alternative approaches that would target unlawful, foreign sites without the collateral damage inflicted by the proposals in H.R. 3261.

For the reasons above, we respectfully ask that you do not cosponsor H.R. 3261. A more detailed and substantive analysis of SOPA's most critical defects and impact on legitimate companies is forthcoming.

Sincerely,