The Next **Killer** App?

BRIEFING KIT

ccia

NetCoalition.com

Supporting Materials

Entrepreneurs’ Opposition Letter on the PROTECT IP Act (September 8, 2011)

Legal Experts’ Opposition Letter on the PROTECT IP Act (July 5, 2011)

Venture Capitalists’ Opposition Letter on the PROTECT IP Act (June 23, 2011)

Public Interest Opposition Letter on the PROTECT IP Act (May 25, 2011)

Net Coalition Opposition Letter on the private right of action provisions included in S.968, the PROTECT IP Act (May 25, 2011)

White Paper on “Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill” (May 2011)

Editorials:

New York Times

Los Angeles Times

OregonLive.com

To Members of the United States Congress:

The undersigned are 130 entrepreneurs, founders, CEOs and executives who have been involved in 283 technology start-ups, and who have created over 50,000 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

[1] See John Haitiwanger et al, Who Creates Jobs? Small vs. Large vs. Young, *US Census Bureau Center for Economic Studies Paper No. CES-WP- 10-17* (August 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1666157&

[2] See McKinsey Global Institute, Internet Matters (May 2011), available at http://www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf

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

[3] Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill" http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf

Will Aldrich
SurveyMonkey, TripIt, Yahoo

Courtland Allen
Syphir, Tyrant

Jean Aw
NOTCOT Inc.

Andy Baio
Upcoming, Kickstarter

Edward Baker
Friend.ly

Jonathan Baudanza
beatlab.com, Rupture

Katia Beauchamp
Birchbox

Idan Beck
Incident Technologies

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

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

Jennifer Dulski
The Dealmap

Rod Ebrahimi
ReadyForZero, DirectHost

Chas Edwards
Luminate, Digg, Federated Media, MySimon

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

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

Eva Ho
Factual, Navigating Cancer, Applied Semantics

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

Ben Ifeld
Macer Media

Jason Jacobs
FitnessKeeper

Daniel James
Three Rings Design

David Jilk
Standing Cloud, eCortex, Xaffire

Noah Kagan
Appsumo, GetGambit

Jon Karl
iovation, ieLogic

Michael Karnjanaprakorn
Skillshare

Bryan Kennedy
Sincerely.com, AppNinjas, Xobni, Pairwise

Derek Kerton
Kerton Group, Telecom Council of Silicon Valley

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

Eric Koger
ModCloth

Kitty Kolding
elicit, House Party, Jupiter

Brian Krausz
GazeHawk

Ryan Lackey
HavenCo, Blue Iraq, Cryptoseal

Jeff Lawson
Twilio, Nine Star, Stubhub, Versity

Peter Lehrman
AxialMarket, Gerson Lehrman Group

Michael Lewis
Stellar Semiconductor, Cryptic Studios

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

Dave Morgan
Simulmedia, TACODA, Real Media

Zac Morris
Caffeinated Mind Inc.

Rick Morrison
Comprehend Systems

Darren Nix
Silver Financial

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

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

Chris Poole
4chan, Canvas

Jon Pospischil
PowerSportsStore, AppMentor, FoodTrux, Custora

Jeff Powers
Occipital

Scott Rafer

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

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

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

Khoi Vinh
Lascaux, NYTimes.com, Behavior Design

Joseph Walla
HelloFax

Brian Walsh
Castfire, Three Deep

David Weekly
PBWorks

Evan Williams
Blogger, Twitter, Obvious

Holmes Wilson
Worchester 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.

Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011"

(PROTECT-IP Act of 2011, S. 968)

July 5, 2011

To Members of the United States Congress:

The undersigned are 108 professors from 31 states, the District of Columbia, and Puerto Rico who teach and write about intellectual property, Internet law, innovation, and the First Amendment. We strongly urge the members of Congress to reject the PROTECT-IP Act (the "Act"). Although the problems the Act attempts to address – online copyright and trademark infringement – are serious ones presenting new and difficult enforcement challenges, the approach taken in the Act has grave constitutional infirmities, potentially dangerous consequences for the stability and security of the Internet's addressing system, and will undermine United States foreign policy and strong support of free expression on the Internet around the world.

The Act would allow the government to break the Internet addressing system. It requires Internet service providers, and operators of Internet name servers, to refuse to recognize Internet domains that a court considers "dedicated to infringing activities." But rather than wait until a Web site is actually judged infringing before imposing the equivalent of an Internet death penalty, the Act would allow courts to order any Internet service provider to stop recognizing the site even on a temporary restraining order or preliminary injunction issued the same day the complaint is filed. Courts could issue such an order even if the owner of that domain name was never given notice that a case against it had been filed at all.

The Act goes still further. It requires credit card providers, advertisers, and search engines to refuse to deal with the owners of such sites. For example, search engines are required to "(i) remove or disable access to the Internet site associated with the domain name set forth in the court order; or (ii) not serve a hypertext link to such Internet site." In the case of credit card companies and advertisers, they must stop doing business not only with sites the government has chosen to sue but any site that a private copyright or trademark owner claims is predominantly infringing. Giving this enormous new power not just to the government but to any copyright and trademark owner would not only disrupt the operations of the allegedly infringing web site without a final judgment of wrongdoing, but would make it extraordinarily difficult for advertisers and credit card companies to do business on the Internet.

Remarkably, the bill applies to domain names outside the United States, even if they are registered not in the .com but, say, the .uk or .fr domains. It even applies to sites that have no connection with the United States at all, so long as they allegedly "harm holders" of US intellectual property rights.

The proposed Act has three major problems that require its rejection:

1. **Suppressing speech without notice and a proper hearing**: The Supreme Court has made it abundantly clear that governmental action to suppress speech taken prior to "a prompt *final judicial decision . . . in an adversary proceeding*" that the speech is unlawful is a presumptively unconstitutional "prior restraint,"[1] the "most serious and the least tolerable infringement on First Amendment rights,"[2] permissible only in the narrowest range of circumstances. The Constitution "require[s] a court, *before* material

[1] *Freedman v. Maryland,* 380 U.S. 51, 58-60 (U.S. 1965) (statute requiring theater owner to receive a license before exhibiting allegedly obscene film was unconstitutional because the statute did not "assure a prompt final judicial decision" that the film was obscene); *see also Bantam Books v. Sullivan*, 372 U.S. 58 (1962) (State Commission's letters suggesting removal of books already in circulation is a "prior administrative restraint" and unconstitutional because there was no procedure for "an almost immediate judicial determination of the validity of the restraint"); *Fort Wayne Books, Inc. v. Indiana,* 489 U.S. 46, 51-63 (1989) (procedure allowing courts to order pre-trial seizure of allegedly obscene films based upon a finding of probable cause was an unconstitutional prior restraint; publications "may not be taken out of circulation completely until there has been a determination of [unlawful speech] after an adversary hearing."). *See also Center For Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004) (statute blocking access to particular domain names and IP addresses an unconstitutional prior restraint).

[2] *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976).

is completely removed from circulation, . . . to make *a final determination* that material is [unlawful] *after an adversary hearing."*[3]

The Act fails this Constitutional test. It authorizes courts to take websites "out of circulation" – to make them unreachable by and invisible to Internet users in the United States and abroad -- immediately upon application by the Attorney General after an *ex parte* hearing. No provision is made for any review of a judge's *ex parte* determination, let alone for a "prompt and final judicial determination, after an adversary proceeding," that the website in question contains unlawful material. This falls far short of what the Constitution requires before speech can be eliminated from public circulation.[4]

2. **Breaking the Internet's infrastructure**: If the government uses the power to demand that individual Internet service providers make individual, country-specific decisions about who can find what on the Internet, the interconnection principle at the very heart of the Internet is at risk. The Internet's Domain Name System ("DNS") is a foundational building block upon which the Internet has been built and on which its continued functioning critically depends. The Act will have potentially catastrophic consequences for the stability and security of the DNS. By authorizing courts to order the removal or replacement of database entries from domain name servers and domain name registries, the Act undermines the principle of domain name universality – that all domain name servers, wherever they may be located on the network, will return the

[3] *CDT v. Pappert*, 337 F.Supp.2d, at 657 (emphasis added).

[4] The Act would also suppress vast amounts of protected speech containing no infringing content whatsoever, and is unconstitutional on that ground as well. The current architecture of the Internet permits large numbers of independent individual websites to operate under a single domain name by the use of unique sub-domains; indeed, many web hosting services operate hundreds or thousands of websites under a single domain name (*e.g.,* www.aol.com, www.terra.es, www.blogspot.com). By requiring suppression of all sub-domains associated with a single offending domain name, the Act "burns down the house to roast the pig," *ACLU v. Reno,* 521 U.S. 844, 882 (1997), failing the fundamental requirement imposed by the First Amendment that it implement the "*least restrictive means* of advancing a compelling state interest." *ACLU v. Ashcroft,* 322 F.3d 240, 251 (3d Cir. 2003) (quoting *Sable Commun. v. FCC*, 492 U.S. at 126 (emphasis added)); *cf. O'Brien*, 391 U.S. at 377 (even the lower "intermediate scrutiny" standard requires that any "incidental restriction on First Amendment freedoms . . . be *no greater than is essential* to the furtherance of that interest"); *see also CDT v Pappert*, 337 F.Supp.2d, at 649 (domain name blocking ["DNS filtering"] resulted in unconstitutional "overblocking" of protected speech whenever "the method is used to block a web site on an online community or a Web Hosting Service, or a web host that hosts web sites as sub-pages under a single domain name," and noting that one service provider "blocked hundreds of thousands of web sites unrelated to" the targeted unlawful conduct); *see also id*., at 640 (statute resulted in blocking fewer than 400 websites containing unlawful child pornography but in excess of *one million websites without any unlawful material*).

same answer when queried with respect to the Internet address of any specific domain name – on which countless numbers of Internet applications, at present, are based. Even more troubling, the Act will critically subvert efforts currently underway – and strongly supported by the U.S. government – to build more robust security protections into the DNS protocols; in the words of a number of leading technology experts, several of whom have been intimately involved in the creation and continued evolution of the DNS for decades:

> The DNS is central to the operation, usability, and scalability of the Internet; almost every other protocol relies on DNS resolution to operate correctly. It is among a handful of protocols that that are the core upon which the Internet is built. . . . Mandated DNS filtering [as authorized by the Act] would be minimally effective and would present technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network. . . . PROTECT IP's DNS filtering will be evaded through trivial and often automated changes through easily accessible and installed software plugins. Given this strong potential for evasion, the long-term benefits of using mandated DNS filtering to combat infringement seem modest at best.[5]

Moreover, the practical effect of the Act would be to kill innovation by new technology companies in the media space. Anyone who starts such a company is at risk of having their source of customers and revenue – indeed, their website itself -- disappear at a moment's notice. The Act's draconian obligations foisted on Internet service providers, financial services firms, advertisers, and search engines, which will have to consult an ever-growing list of prohibited sites they are not allowed to connect to or do business with, will further hamper the Internet's operations and effectiveness.

[5] Crocker, et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," available at http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf. The authors describe in detail how implementation of the Act's mandatory DNS filtering scheme will conflict with and undermine development of the "DNS Security Extensions," a "critical set of security updates" for the DNS under development (with the strong support of both the U.S. government and private industry) since the mid-1990s.

3. **<u>Undermining United States' leadership in supporting and defending free speech and the free exchange of information on the Internet</u>**: The Act represents a retreat from the United States' strong support of freedom of expression and the free exchange of information and ideas on the Internet. At a time when many foreign governments have dramatically stepped up their efforts to censor Internet communications,[6] the Act would incorporate into U.S. law – for the first time – a principle more closely associated with those repressive regimes: a right to insist on the removal of content from the global Internet, regardless of where it may have originated or be located, in service of the exigencies of domestic law. China, for example, has (justly) been criticized for blocking free access to the Internet with its Great Firewall. But even China doesn't demand that search engines outside China refuse to index or link to other Web sites outside China. The Act does just that.

The United States has been the world's leader, not just in word but in deed, in codifying these principles of speech and exchange of information. Requiring Internet service providers, website operators, search engine providers, credit card companies and other financial intermediaries, and Internet advertisers to block access to websites because of their content would constitute a dramatic retreat from the United States' long-standing policy, implemented in section 230 of the Communications Decency Act, section 512 of the Copyright Act, and elsewhere, of allowing Internet intermediaries to focus on empowering communications by and among users, free from the need to

[6] Secretary of State Clinton, in her "Remarks on Internet Freedom" delivered earlier this year, put it this way:

> In the last year, we've seen a spike in threats to the free flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. In Vietnam, access to popular social networking sites has suddenly disappeared. And last Friday in Egypt, 30 bloggers and activists were detained. . . . As I speak to you today, government censors somewhere are working furiously to erase my words from the records of history. But history itself has already condemned these tactics.
>
> [T]he new iconic infrastructure of our age is the Internet. Instead of division, it stands for connection. But even as networks spread to nations around the globe, virtual walls are cropping up in place of visible walls. . . . Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. . . . With the spread of these restrictive practices, a new information curtain is descending across much of the world.

monitor, supervise, or play any other gatekeeping or policing role with respect to those communications. These laws represent the hallmark of United States leadership in defending speech and their protections are significantly responsible for making the Internet into the revolutionary communications medium that it is today. They reflect a policy that has not only helped make the United States the world leader in a wide range of Internet-related industries, but it has also enabled the Internet's uniquely decentralized structure to serve as a global platform for innovation, speech, collaboration, civic engagement, and economic growth. The Act would undermine that leadership and dramatically diminish the Internet's capability to be a functioning communications medium. In conclusion, passage of the Act will compromise our ability to defend the principle of the single global Internet – the Internet that looks the same to, and allows free and unfettered communication between, users located in Boston and Bucharest, free of locally-imposed censorship regimes. As such, it may represent the biggest threat to the Internet in its history.

While copyright infringement on the Internet is a very real problem, copyright owners already have an ample array of tools at their disposal to deal with the problem. We shouldn't add the power to break the Internet to that list.

Signed,[7]

Professor John R. Allison
McCombs School of Business
University of Texas at Austin

Professor Brook K. Baker
Northeastern University School of Law

Professor Derek E. Bambauer
Brooklyn Law School

Professor Margreth Barrett
Hastings College of Law
University of California-San Francisco

Professor Mark Bartholomew
University at Buffalo Law School

[7] All institutions are listed for identification purposes only.

Professor Ann M. Bartow
Pace Law School

Professor Marsha Baum
University of New Mexico School of Law

Professor Yochai Benkler
Harvard Law School

Professor Oren Bracha
University of Texas School of Law

Professor Annemarie Bridy
University of Idaho College of Law

Professor Dan L. Burk
University of California-Irvine School of Law

Professor Irene Calboli
Marquette University School of Law

Professor Adam Candeub
Michigan State University College of Law

Professor Michael Carrier
Rutgers Law School – Camden

Professor Michael W. Carroll
Washington College of Law
American University

Professor Brian W. Carver
School of Information
University of California-Berkeley

Professor Anupam Chander
University of California-Davis School of Law

Professor Andrew Chin
University of North Carolina School of Law

Professor Ralph D. Clifford
University of Massachusetts School of Law

Professor Julie E. Cohen
Georgetown University Law Center

Professor G. Marcus Cole
Stanford Law School

Professor Kevin Collins
Washington University-St. Louis School of Law

Professor Danielle M. Conway
University of Hawai'i Richardson School of Law

Professor Dennis S. Corgill
St. Thomas University School of Law

Professor Christopher A. Cotropia
University of Richmond School of Law

Professor Thomas Cotter
University of Minnesota School of Law

Professor Julie Cromer Young
Thomas Jefferson School of Law

Professor Ben Depoorter
Hastings College of Law
University of California – San Francisco

Professor Eric B. Easton
University of Baltimore School of Law

Anthony Falzone
Director, Fair Use Project
Stanford Law School

Professor Nita Farahany
Vanderbilt Law School

Professor Thomas G. Field, Jr.
University of New Hampshire School of Law

Professor Sean Flynn
Washington College of Law
American University

Professor Brett M. Frischmann
Cardozo Law School
Yeshiva University

Professor Jeanne C. Fromer
Fordham Law School

Professor William T. Gallagher
Golden Gate University School of Law

Professor Laura N. Gasaway
University of North Carolina School of Law

Professor Deborah Gerhardt
University of North Carolina School of Law

Professor Llew Gibbons
University of Toledo College of Law

Professor Eric Goldman
Santa Clara University School of Law

Professor Marc Greenberg
Golden Gate University School of Law

Professor James Grimmelman
New York Law School

Professor Leah Chan Grinvald
St. Louis University School of Law

Professor Richard Gruner
John Marshall Law School

Professor Bronwyn H. Hall
Haas School of Business
University of California at Berkeley

Professor Robert A. Heverly
Albany Law School
Union University

Professor Laura A. Heymann
Marshall-Wythe School of Law
College of William & Mary

Professor Herbert Hovenkamp
University of Iowa College of Law

Professor Dan Hunter

New York Law School

Professor David R. Johnson
New York Law School

Professor Faye E. Jones
Florida State University College of Law

Professor Amy Kapczynski
University of California-Berkeley Law School

Professor Dennis S. Karjala
Arizona State University College of Law

Professor Anne Klinefelter
University of North Carolina College of Law

Professor Mary LaFrance
William Boyd Law School
University of Nevada – Las Vegas

Professor Amy L. Landers
McGeorge Law School
University of the Pacific

Professor Mark Lemley
Stanford Law School

Professor Lawrence Lessig
Harvard Law School

Professor David S. Levine
Elon University School of Law

Professor Yvette Joy Liebesman
St. Louis University School of Law

Professor Lydia Pallas Loren
Lewis & Clark Law School

Professor Michael J. Madison
University of Pittsburgh School of Law

Professor Gregory P. Magarian
Washington University-St. Louis School of Law

Professor Phil Malone
Harvard Law School

Professor Christian E. Mammen
Hastings College of Law
University of California-San Francisco

Professor Jonathan Masur
University of Chicago Law School

Professor Andrea Matwyshyn
Wharton School of Business
University of Pennsylvania
Professor J. Thomas McCarthy
University of San Francisco School of Law

Professor William McGeveran
University of Minnesota Law School

Professor Stephen McJohn
Suffolk University Law School

Professor Mark P. McKenna
Notre Dame Law School

Professor Hiram Melendez-Juarbe
University of Puerto Rico School of Law

Professor Viva Moffat
University of Denver College of Law

Professor Ira Nathenson
St. Thomas University School of Law

Professor Tyler T. Ochoa
Santa Clara University School of Law

Professor David S. Olson
Boston College Law School

Professor Barak Y. Orbach
University of Arizona College of Law

Professor Kristen Osenga
University of Richmond School of Law

Professor Aaron Perzanowski

Wayne State University Law School

Malla Pollack
Co-author, Callman on Trademarks, Unfair Competition, and Monopolies

Professor David G. Post
Temple University School of Law

Professor Connie Davis Powell
Baylor University School of Law

Professor Margaret Jane Radin
University of Michigan Law School

Professor Glenn Reynolds
University of Tennessee Law School

Professor David A. Rice
Roger Williams University School of Law

Professor Neil Richards
Washington University-St. Louis School of Law

Professor Michael Risch
Villanova Law School

Professor Betsy Rosenblatt
Whittier Law School

Professor Matthew Sag
Loyola University-Chicago School of Law

Professor Pamela Samuelson
University of California-Berkeley Law School

Professor Sharon K. Sandeen
Hamline University School of Law

Professor Jason M. Schultz
UC Berkeley Law School

Professor Jeremy Sheff
St. John's University School of Law

Professor Jessica Silbey
Suffolk University Law School

Professor Brenda M. Simon
Thomas Jefferson School of Law

Professor David E. Sorkin
John Marshall Law School

Professor Christopher Jon Sprigman
University of Virginia School of Law

Professor Katherine J. Strandburg
NYU Law School

Professor Madhavi Sunder
University of California-Davis School of Law

Professor Rebecca Tushnet
Georgetown University Law Center

Professor Deborah Tussey
Oklahoma City University School of Law

Professor Barbara van Schewick
Stanford Law School

Professor Eugene Volokh
UCLA School of Law

Professor Sarah K. Wiant
William & Mary Law School

Professor Darryl C. Wilson
Stetson University College of Law

Professor Jane K. Winn
University of Washington School of Law

Professor Peter K. Yu
Drake University Law School

Professor Tim Zick
William & Mary Law School

Venture Capitalists’ Opposition Letter on the PROTECT IP Act

return to Supporting Materials

Thursday, June 23, 2011

Members of the U.S. Congress,

We write to express our concern with S. 968, the PROTECT IP Act (“PIPA”). As investors in technology companies, we agree with the goal of fostering a thriving digital content market online. Unfortunately, the current bill will not only fail to achieve that goal, it will stifle investment in Internet services, throttle innovation, and hurt American competitiveness.

Online innovation has flourished, in part, because the Digital Millennium Copyright Act (DMCA), though flawed, created clear, defined safe harbors for online intermediaries. The DMCA creates legal certainty and predictability for online services -- so long as they meet the conditions of the safe harbors, including an appropriate notice-and- takedown policy, they have no liability for the acts of their users. At the same time, the DMCA gives rights-holders a way to take down specific infringing content, and it is working well.

We appreciate PIPA’s goal of combating sites truly dedicated to infringing activity, but it would undermine the delicate balance of the DMCA and threaten legitimate innovation. The bill is ripe for abuse, as it allows rights-holders to require third-parties to block access to and take away revenues sources for online services, with limited oversight and due process.

In particular:

1. By requiring “information location tools” -- potentially encompassing any "director[ies], index[es], reference[s], pointer[s], or hypertext link[s]” -- to remove access to entire domains, the bill puts burdens on countless Internet services.

2. By requiring access to sites to be blocked by Domain Name System providers, it endangers the security and integrity of the Internet.

3. The bill’s private right of action will no doubt be used by many rights-holders in ways that create significant burdens on legitimate online commerce services. The scope of orders and cost of litigation could be significant, even for companies acting in good faith. Rights-holders have stated their interest in this private right of action because they worry that the Department of Justice will not have enough resources to initiate actions against all of

> the infringing sites. Yet, why should costs be shifted to innocent Internet entrepreneurs, most of whom have budgets smaller than the Department of Justice's?

While we understand PIPA was originally intended to deal with "rogue" foreign sites, we think PIPA will ultimately put American innovators and investors at a clear disadvantage in the global economy. For one, services dedicated to infringement will simply make their sites easy to find and access in other ways, and determined users who want to find blocked content will simply shift to services outside the reach of U.S. law, in turn giving a leg up to foreign search engines, DNS providers, social networks, and others. Second, PIPA creates a dangerous precedent and a convenient excuse for countries to engage in protectionism and censorship against U.S. services. These countries will point to PIPA as precedent for taking action against U.S. technology and Internet companies.

The entire set of issues surrounding copyright in an increasingly digital world are extremely complex, and there are no simple solutions. These challenges are best addressed by imagining, inventing, and financing new models and new services that will allow creative activities to thrive in the digital world. There is a new model for financing, distributing, and profiting from copyrighted material and it is working -- just look at services like iTunes, Netflix, Pandora, Kickstarter, and more. Pirate web sites will always exist, but if rights holders make it easy to get their works through innovative Internet models, they can and will have bright futures.

Congress should not chill investment and reduce incentives to work on private sector solutions. Instead, we encourage Congress to focus on making it easier to license works and bring new, innovative services to market.

Sincerely,

Marc Andreessen, Andreessen Horowitz
Brady Bohrmann, Avalon Ventures
John Borthwick, Betaworks
Mike Brown, Jr., AOL Ventures
Brad Burnham, Union Square Ventures
Jeffrey Bussgang, Flybridge Capital Partners
John Buttrick, Union Square Ventures
Randy Castleman, Court Square Ventures
Tony Conrad, True Ventures
Ron Conway, SV Angel

Chris Dixon, Founder Collective
Bill Draper, Draper Richards
Esther Dyson, EDventure Holdings
Roger Ehrenberg, IA Ventures
Brad Feld, Foundry Group
Peter Fenton, Benchmark Capital
Ron Fisher, Softbank Capital
Chris Fralic, First Round Capital
David Frankel, Founder Collective
Ric Fulop, North Bridge
Brad Gillespie, IA Ventures
Allen "Pete" Grum, Rand Capital
Chip Hazard, Flybridge Capital Partners
Rick Heitzmann, FirstMark Capital
Eric Hippeau, Lerer Ventures
Reid Hoffman, Greylock Partners
Ben Horowitz, Andreessen Horowitz
Mark Jacobsen, OATV
Amish Jani, First Mark Capital
Brian Kempner, First Mark Capital
Vinod Khosla, Khosla Ventures
Josh Kopelman, First Round Capital
David Lee, SV Angel
Lawrence Lenihan, FirstMark Capital
Kenneth Lerer, Lerer Ventures
Jordan Levy, Softbank Capital
Jason Mendelson, Foundry Group
R. Ann Miura-Ko, Floodgate
Howard Morgan, First Round Capital
John O'Farrell, Andreessen Horowitz
Tim O'Reilly, OATV
David Pakman, Venrock
Eric Paley, Founder Collective
Alan Patricof, Greycroft Partners
Danny Rimer, Index Ventures
Neil Rimer, Index Ventures
Bryce Roberts, OATV
Bijan Sabet, Spark Capital
David Sze, Greylock Partners
Andrew Weissman, Betaworks

Albert Wenger, Union Square Ventures
Eric Wiesen, RRE Ventures
Fred Wilson, Union Square Ventures

May 25, 2011

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

The Honorable Chuck Grassley
Ranking Member
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: S. 968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011

Dear Chairman Leahy and Ranking Member Grassley:

Although the undersigned entities harbor no sympathy for websites whose primary purpose is to sell illegal products online, we cannot support S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, in its current form. The legislation has been improved over its predecessor with the removal of provisions targeting domain name registries and registrars, and with the narrowing of certain definitions to avoid some of the overbreadth issues inherent in the Combating Online Infringement and Counterfeits Act. We appreciate your work on these matters. Nonetheless, certain provisions within S. 968 continue to threaten the stability, freedom, and economic potential of the Internet.

The new legislation maintains the provision to direct Internet Service Providers (ISPs) and others to interfere with Domain Name System (DNS) lookup services by tampering with their DNS responses. We continue to believe that such a provision would be ineffective and runs contrary to the US government's commitment to advancing a single, global Internet. Its inclusion risks setting a precedent for other countries, even democratic ones, to use DNS mechanisms to enforce a range of domestic policies, erecting barriers on the global medium of the Internet. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association. In addition, circumventing DNS blocking risks substantial collateral damage by making domestic networks and users more vulnerable to cybersecurity attacks, and would increase opportunities for identity theft as users migrate to offshore DNS providers not subject to S. 968. It is critical that the Committee, before endorsing such a change to U.S. law, explore whether DNS blocking would likely result in a sufficient decrease in for-profit Internet piracy to justify taking such risks.

Furthermore, the new inclusion of "information location tools" (also referred to as the "search engine" portion of the bill) has expanded the legislation's reach. The term "information location tools" appears to encompass "director[ies], index[es], reference[s], pointer[s], or hypertext link[s]." With this provision in place, S. 968 makes nearly every actor on the Internet potentially subject to enforcement orders under the bill, raising new policy questions regarding government interference with online activity and speech.

We continue to urge the Committee to proceed cautiously given the concerns of the undersigned and we look forward to working with you and your colleagues in a constructive manner on improving S. 968.

Sincerely,

American Association of Law Libraries

Association of College and Research

Libraries American Library Association

Association of Research Libraries

Center for Democracy and

Technology Demand Progress

EDUCAUSE

Electronic Frontier Foundation

Human Rights Watch

Rebecca MacKinnon, Bernard Schwartz Senior Fellow, New America Foundation

Public Knowledge

Reporters sans frontières / Reporters Without Borders

Special Libraries Association

Net Coalition Opposition Letter on the *private right of action* provisions included in S.968, the PROTECT IP Act

return to Supporting Materials

May 25, 2011

The Honorable Patrick J. Leahy
Chairman
United States Senate
Committee on the Judiciary
437 Russell Senate Building
Washington, DC 20510

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

Dear Chairman Leahy and Ranking Member Grassley:

The undersigned below support the goals of S. 968, the PROTECT IP Act, to enforce intellectual property rights effectively by addressing rampant infringement by web sites designed and operated to promote and profit from illegal activities. While we each share that goal, and each continue to have concerns with various specific provisions in the legislation, our purpose in this letter is to express in clear terms our serious concerns with the private right of action provisions included in S. 968. The private right of action should be removed from the legislation.

Under the current version of the PROTECT IP Act, an owner of a copyright or trademark could bring an action against a domain name associated with a website dedicated to infringing activity. It is reasonable to expect that a very large number of such actions will be brought, and in many cases, especially with non-U.S. domain names, the domain name owner will not respond to the complaint. It is very likely in such cases with only one party present that courts will enter default judgments and declare that the targeted websites are dedicated to infringing activity. The IP owner will then be able to ask the court to issue an order directed at two categories of services providers. First, a payment system could be required to stop processing transactions between the website and U.S. customers. Second, an advertising network could be directed to stop placing ads on the website.

We believe that the currently proposed private litigation-based process will, however unintentionally, become a one-sided litigation machine with rights owners mass-producing virtually identical cases against foreign domain names for the purpose of obtaining orders to serve on U.S. payment and advertising companies. Not only do we believe that this will be a significant driver of new litigation in federal courts, and will result in an endless stream of court orders imposing duties on U.S.-based companies, but we also believe that this litigation-based regime will significantly reduce the incentive that rights owners have to participate in a cooperative manner in the processes created by payment and advertising companies to address illegal activities by third parties. We are confident that upon further review you will not support creating a private litigation regime that appears so open to abuse and which will undermine the prospects for private sector cooperation.

Along with the fact that the private right of action regime will likely lead to a new litigation industry aimed at obtaining court orders related to websites whose owners will not appear in U.S. courts, we also believe that the regime will lead to private actions against US payment and advertising companies. It is likely that the operators of websites that are the target of court decisions and therefore the court orders aimed at payment and advertising companies will respond by attempting to circumvent the "blocks" imposed by payment systems and advertising networks. S. 968 authorizes the IP owner to bring private enforcement action against the payment and advertising service providers to compel compliance with an order, and the service provider could find itself enmeshed in litigation based on the actions of the suspected infringers of which it has no knowledge.

To prevail in an enforcement action against a service provider, the IP owner would have to demonstrate that the service provider knowingly and willfully failed to comply with an order. The IP owner could argue that the service provider knew that its blocks could be circumvented, and thus that its failure to monitor the site and respond on its own to each act of circumvention constituted a violation of the order.

Regardless of the validity of this argument, the cost of litigation, including discovery about the service provider's operations and its awareness of the activities of the website at issue, might be sufficient to force the service providers to settle the claim on terms very favorable to the IP owner. Several law firms representing IP owners such as publishers of pornography have learned how to "game" the copyright system, and the private right of action under S. 968 provides them with an additional weapon.

Moreover, even if most IP owners do not use the threat of enforcement actions to extort payments from service providers, the IP owners can employ such actions to shift the burden of monitoring websites subject to orders to the service providers. Given the large number of IP owners and infringing websites, and the relatively small number of major payment systems and advertising networks, the service providers' monitoring costs could be significant.

Last year's version of this legislation allowed only an action by the Attorney General. S. 968, by contrast, allows both an AG action and a private action. To prevent the abuses described above while still accomplishing the bill's legitimate objectives, the private right of action should be removed, leaving the AG action.

Respectfully,

American Express Company
Consumer Electronics Association
Discover

Visa PayPal
NetCoalition
Yahoo!
eBay
Google

Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill

May 2011

Authors: Steve Crocker, Shinkuro, Inc.
David Dagon, Georgia Tech
Dan Kaminsky, DKH
Danny McPherson, Verisign, Inc.
Paul Vixie, Internet Systems Consortium

Affiliations provided for identification only
Brief biographies of authors available below

EXECUTIVE SUMMARY

This paper describes technical problems raised by the DNS filtering requirements in S. 978, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act"). Its authors come from the technical, operational, academic, and research communities. We are leading domain name system (DNS) designers, operators, and researchers, who have created numerous "RFCs" (technical design documents) for DNS, published many peer-reviewed academic studies relating to architecture and security of the DNS, and operate important DNS infrastructure on the Internet.

The authors of this paper take no issue with strong enforcement of intellectual property rights generally. The DNS filtering requirements in the PROTECT IP Act, however, raise serious technical concerns, including:

- The U.S. Government and private industry have identified Internet security and stability as a key part of a wider cyber security strategy, and if implemented, the DNS related provisions of PROTECT IP would weaken this important commitment.
- DNS filters would be evaded easily, and would likely prove ineffective at reducing online infringement. Further, widespread circumvention would threaten the security and stability of the global DNS.
- The DNS provisions would undermine the universality of domain names, which has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet.
- Migration away from ISP-provided DNS servers would harm efforts that rely on DNS data to detect and mitigate security threats and improve network performance.
- Dependencies within the DNS would pose significant risk of collateral damage, with filtering of one domain potentially affecting users' ability to reach non-infringing Internet content.
- The site redirection envisioned in Section 3(d)(II)(A)(ii) is inconsistent with security extensions to the DNS that are known as DNSSEC. The U.S. Government and private industry have identified DNSSEC as a key part of a wider cyber security strategy, and many private, military, and governmental networks have invested in DNSSEC technologies.
- If implemented, this section of the PROTECT IP Act would weaken this important effort to improve Internet security. It would enshrine and institutionalize the very network manipulation that DNSSEC must fight in order to prevent cyberattacks and other malevolent behavior on the global Internet, thereby exposing networks and users to increased security and privacy risks.

We believe the goals of PROTECT IP are important, and can be accomplished without reducing DNS security and stability through strategies such as the non-DNS remedies contained in PROTECT IP and international cooperation.

I. Introduction

The recently introduced PROTECT IP Act of 2011,[1] the successor to last year's COICA legislation,[2] includes a range of proposed new enforcement mechanisms to combat the online infringement of intellectual property. Of keen interest to the community of engineers working on issues related to the domain-name system (DNS) is the DNS filtering provision that would require ISPs and other operators of "non-authoritative DNS servers" to take steps to filter and redirect requests for domains found by courts to point to sites that are dedicated to infringement. This paper seeks to explain a set of technical concerns with mandated DNS filtering and to urge lawmakers to reconsider enacting such a mandate into law.

Combating online infringement of intellectual property is without question an important objective. The authors of this paper take no issue with the lawful removal of infringing content from Internet hosts with due process. But while we support the goals of the bill, we believe that the use of mandated DNS filtering to combat online infringement raises serious technical and security concerns.

Mandated DNS filtering would be minimally effective and would present technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network.

II. DNS Background

The domain-name system, or DNS, is a system that makes the Internet more accessible to humans. When computers on the Internet communicate with each other, they use a series of numbers called "IP addresses" (such as 156.33.195.33) to direct their messages to the correct recipient. These numbers, however, are hard to remember, so the DNS system allows humans to use easier-to-remember words (such as "senate.gov“) to access websites or send e-mail. Such names resolve to the proper IP numbers through the use of domain name servers. These servers are set up in a distributed fashion, often globally, such that resolution of names connected to IP addresses may pass through many servers during Internet data flow.[3] To make the DNS faster and less expensive to operate, over ten million so-called "recursive servers" exist as accelerators of convenience, to store and retransmit DNS data to nearby users. The PROTECT IP Act proposes legal remedies for infringement that would affect the operators of these "recursive

[1] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Congress

[2] Combatting Online Infringements and Counterfeits Act, S. 3480, 111th Congress

[3] *See* P. Mockapetris, RFC 1034, "Domain Names – Concepts and Facilities," Internet Engineering Task Force, November 1987, http://www.ietf.org/rfc/rfc1034.txt.

servers," which are the type of DNS servers used by the computers of end users to resolve DNS names in order to access content on the Internet.[4]

The DNS is central to the operation, usability, and scalability of the Internet; almost every other protocol relies on DNS resolution to operate correctly. It is among a handful of protocols that that are the core upon which the Internet is built. Readers interested in finding out more about the DNS are directed to Paul Vixie's article, "DNS Complexity."[5] See also Appendix A for a pictorial view of the DNS and DNS filtering.

The DNS is a crucial element of Internet communication in part because it allows for "universal naming" of Internet resources. Domain names have in almost all cases been universal, such that a given domain name means the same thing, and is uniformly accessible, no matter from which network or country it is looked up or from which type of device it is accessed.

This universality is assumed by many Internet applications. The domain name given to an Internet device or service is frequently stored and reused, or forwarded to other Internet devices that may not be customers of the same service provider or residents in the same country. For example, web URLs are frequently sent inside electronic mail messages where they are expected to mean the same thing (*i.e.*, to reach the same content) to the recipient of the e-mail that they meant to the sender. Universality of domain names has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet. The importance of universal naming is underscored in the U.S. International Strategy for Cyberspace: "The United States supports an Internet with end-to-end interoperability, which allows people worldwide to connect to knowledge, ideas, and one another through technology that meets their needs."[6]

Mandated DNS filtering by nameservers threatens universal naming by requiring that some nameservers return different results than others for certain domains. While this type of mandated DNS manipulation is reportedly used in some Middle Eastern countries and in the so-called Great Firewall of China, the mandated DNS filtering proposed by PROTECT IP would be unprecedented in the United States and poses some serious concerns as described below.

[4] The other type of DNS server is termed "authoritative." These systems are the DNS servers that are usually under control of the content provider, and that provide the "authoritative" answer as to where on the Internet a given website or service is located. Essentially, "recursive" servers are the DNS servers that help users locate where things are on the Internet, and "authoritative" servers are the DNS servers are the sources of the answers to those queries. Because the focus of the PROTECT IP Act is on recursive DNS servers (and not authoritative servers), the terms "server," and "DNS server," and "resolver" in the remainder of this paper shall mean recursive servers that help users locate content and services on the Internet.

[5] Paul Vixie, "DNS Complexity," *ACM Queue 5*, no. 3, April 2007.

[6] United States Office of the President, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, at page 8.

III. Technical Challenges Raised By Mandatory DNS Filtering

A. DNS Filtering in Tension with DNSSEC

PROTECT IP would empower the Department of Justice, with a court order, to require operators of DNS servers to take steps to filter resolution of queries for certain names. Further, the bill directs the Attorney General to develop a textual notice to which users who attempt to navigate to these names will be redirected.[7] Redirecting users to a resource that does not match what they requested, however, is incompatible with end-to-end implementations of DNS Security Extensions (DNSSEC), a critical set of security updates. Implementing both end-to-end DNSSEC and PROTECT IP redirection orders simply would not work. Moreover, *any* filtering by nameservers, even without redirection, will pose security challenges, as there will be no mechanism to distinguish court-ordered lookup failure from temporary system failure, or even from failure caused by attackers or hostile networks.

Security problems with the DNS were identified over twenty years ago, and the DNSSEC approach to correcting vulnerabilities has been under development since the mid-1990s.[8] In short, DNSSEC allows for DNS records to be cryptographically signed, thereby providing a secure authentication of Internet assets. When implemented end-to-end between authoritative nameservers and requesting applications, DNSSEC prevents man-in-the-middle attacks on DNS queries by allowing for provable authenticity of DNS records and provable inauthenticity of forged data. This secure authentication is critical for combatting the distribution of malware and other problematic Internet behavior. Authentication flaws, including in the DNS, expose personal information, credit card data, e-mails, documents, stock data, and other sensitive information, and represent one of the primary techniques by which hackers break into and harm American assets.

DNSSEC has been promoted and supported by the highest levels of the U.S. government. Development and rollout has involved a major bipartisan political effort, undertaken at great expense as a public/private partnership dating back to the Clinton administration. President George W. Bush included securing the DNS among national cybersecurity priorities as early as 2003.[9] When the root zone trust anchor was published just under a year ago, enabling use of DNSSEC within the global DNS, the Obama administration hailed it as a "major milestone for Internet security."[10] The security of the Internet and the success of DNSSEC have been, and remain, a vital policy goal of the United States.[11]

[7] Section 3(d)(2)(A)(ii), "Text of Notice."

[8] *See* http://www.dnssec.net.

[9] United States Office of the President, *The National Strategy to Secure Cyberspace*, February 2003, *http*://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

[10] Andrew McLaughlin, "A Major Milestone for Internet Security," The White House blog, July 22, 2010, http://www.whitehouse.gov/blog/2010/07/22/a-major-milestone-internet-security.

[11] *See* United States Office of the President, *National Strategy for Trusted Identities in Cyberspace*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*; See also* United States Office of the President, *International Strategy for Cyberspace*, May 2011, *supra*, note 6, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

The fundamental architectural concept behind DNSSEC is that any information associated with a name must verifiably come from the owner of that name. For example, DNSSEC is designed to ensure that if a user requests the mail server for the U.S. Senate, the response is actually the legitimate server to communicate with to send e-mail to addresses within the senate.gov domain. The power of DNSSEC is that it provides a widely deployed and well managed infrastructure that allows only the Senate IT staff to manipulate the authoritative senate.gov nameserver, while only the House of Representative's IT staff can manipulate the authoritative house.gov nameserver.

By mandating redirection, PROTECT IP would require and legitimize the very behavior DNSSEC is designed to detect and suppress. Replacing responses with pointers to other resources, as PROTECT IP would require, is fundamentally incompatible with end-to-end DNSSEC. Quite simply, a DNSSEC-enabled browser or other application cannot accept an unsigned response; doing so would defeat the purpose of secure DNS. Consistent with DNSSEC, the nameserver charged with retrieving responses to a user's DNSSEC queries cannot sign any alternate response in any manner that would enable it to validate a query.

Although DNSSEC-enabled applications are not yet in widespread use, the need for such applications has been a key factor driving DNSSEC's development. Today, applications and services that require security (*e.g.* online banking) rely on other forms of authentication to work around a potentially insecure DNS, but a secure DNS would be more effective and efficient. End-to-end deployment of DNSSEC is required to better secure the sensitive applications we have today and allow for new sensitive applications. A legal mandate to operate DNS servers in a manner inconsistent with end-to-end DNSSEC would therefore interfere with the rollout of this critical security technology and stifle this emerging platform for innovation.

Even DNS filtering that did not contemplate redirection would pose security challenges. The only possible DNSSEC-compliant response to a query for a domain that has been ordered to be filtered is for the lookup to fail. It cannot provide a false response pointing to another resource or indicate that the domain does not exist. From an operational standpoint, a resolution failure from a nameserver subject to a court order and from a hacked nameserver would be indistinguishable. Users running secure applications have a need to distinguish between policy-based failures and failures caused, for example, by the presence of an attack or a hostile network, or else downgrade attacks would likely be prolific.[12]

DNSSEC is being implemented to allow systems to demand verification of what they get from the DNS. PROTECT IP would not only require DNS responses that cannot deliver such proof, but it would enshrine and institutionalize the very network manipulation DNSSEC must fight in order to prevent cyberattacks and other miscreant behavior on the global Internet.

[12] If two or more levels of security exist in a system, an attacker will have the ability to force a "downgrade" move from a more secure system function or capability to a less secure function by making it appear as though some party in the transaction doesn't support the higher level of security. Forcing failure of DNSSEC requests is one way to effect this exploit, if the attacked system will then accept forged insecure DNS responses. To prevent downgrade attempts, systems must be able to distinguish between legitimate failure and malicious failure.

B. The Proposed DNS Filters Would Be Circumvented Easily

As described above, the DNS was adopted to achieve universal naming for Internet resources. The fact that host names resolve consistently regardless of which network performs the request is a key factor in the Internet's success as a global communications network. Anybody who has surfed to a site in a public place, an office, or someone else's house, and gone to a site different from what he or she is used to at home, will understand frustrations that can come from filtering. To the extent that the naming system becomes less universal or consistent, the economic and social value of the network will suffer.

DNS filtering does not remove or prevent access to Internet content. It simply prevents resolution by a particular DNS server of a filtered domain to its associated IP address. The offending site remains available and accessible through non-filtered nameservers or numerous other means, including direct accessibility from the client to the server if they have the corresponding information. Circumvention is possible, with increasing ease, and is quite likely in the case of attempts to filter infringement via the DNS. All of the methods that we discuss in this section pose risks to the security and stability of the DNS, and to broader societal concerns.

Evidence from the recent domain seizures by U.S. Immigrations and Customs Enforcement demonstrates how likely circumvention is to occur. Data captured by Arbor Networks regarding the seizure of TVShack.net, showed what appeared to be only a short term impact on actual traffic to the pirates' servers.[13] The content simply was moved to a different domain, with little long-term impact likely. Similarly, Alexa traffic rankings indicate that traffic to rojadirecta.es, the replacement for the seized rojadirecta.com, quickly reached levels comparable to that of the former domain.[14] This occurred due to the fact that users and infringing websites do not simply "give up" in response to implementation of a filtering mechanism. They go online, find new (non-American) domains or direct IP numbers, and connect as they usually would.

In the case of DNS filtering, users need not navigate to new domains, but can instead simply use non-filtered DNS servers. To understand this approach, it is helpful to understand what normally occurs for most residential broadband customer installations. Normally, as part of the initial settings provided by ISPs to their customers, the ISPs select the users' DNS server (commonly as part of dynamic addressing lease negotiation or in setting up a user's equipment). In general, the operator-selected DNS server is local to the user, providing fast, efficient resolution. Thus, for example, Comcast customers generally use Comcast's DNS servers allowing for an "accelerated," and topologically optimal, DNS experience.

However, users may change their DNS server settings, either by running a local resolver or by updating a single OS configuration parameter. Moreover, applications and even websites can also change a users' DNS settings automatically. A 2008 survey using data from Google found that hundreds of malware websites automatically change the DNS settings of users who simply

[13] Craig Labovtiz, "Takedown," Arbor Networks blog, July 2, 2010, http://asert.arbornetworks.com/2010/07/takedown/

[14] Compare http://www.alexa.com/siteinfo/rojadirecta.com# and http://www.alexa.com/siteinfo/rojadirecta.es#.

visit a malicious web site.[15] It is likely, if not inevitable, that infringement sites would use the same strategy, allowing a single site to instantly, silently, and permanently change a user's DNS path and evade DNS filtration and filtering.

How easily could software make such a change? Just a single line of code is needed to change one registry key in Microsoft Windows. As documented widely by Microsoft itself, software merely needs to edit one system registry parameter:

```
        \\HKLM\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters
```
[16]

Such behavior is common. In a survey of 100,000 malware samples, pulled at random from the Georgia Institute of Technology's malware repository, over 98% were found to read Windows registry settings, and some 68% were found to change the registry. Indeed, the anti-malware industry even has a term for viruses that specifically manipulate resolution via registry keys: "DNS-changers", or "DNS-changing malware," and such techniques have been employed by miscreants for nearly a decade.[17]

The choice of alternative DNS servers is effectively unlimited. In the same study, a survey of so-called "open-recursive" DNS resolvers revealed a dramatic increase in the number of public DNS servers. At present, there are *tens of millions* of open, public DNS servers, many outside the U.S. Sites offering or promoting the downloading of copyright-infringing content could use almost any of these resolvers to evade domestic DNS filtering.

An obvious possibility would be for the operators of the infringement sites themselves to operate alternative DNS servers for their users. It has been suggested that perhaps pirate sites would not wish to operate such a service because it would be difficult or expensive. However, DNS resolvers are lightweight and do not expose the same network engineering profile or carry the same costs as other circumvention technologies such as full-traffic encryption. In practice, a $1,000 server can respond to over 100,000 DNS requests *per second*. It is substantially easier to provide the handful of bits required for a DNS response than to expose a complex searchable web interface to pirated content. Realistically, the DNS accelerating service could be provided at no additional cost, using spare capacity on existing servers. Thus, those entities large enough to attract the attention of PROTECT IP likely will be large enough to handle the DNS load of their user base.

Suggestions have been made that U.S. users will not use servers located outside of the United States because the nameservers are foreign and untrusted.[18] The user who is seeking pirated content, however, will often be more concerned about getting the content than with how reputable a particular DNS provider might be. More importantly, in many cases, the user will

[15] D. Dagon, N. Provos, C. P. Lee, and W. Lee, "Corrupted DNS resolution paths: The rise of a malicious resolution authority," In *Proceedings of Network and Distributed Security Symposium* (NDSS '08), 2008. Note: The 2008 study and this report share an author.

[16] Microsoft, Inc. DNS Registry Entries. http://technet.microsoft. com/en-us/library/dd197418%28WS.10%29.aspx, 2011.

[17] Dagon et. al., "Corrupted DNS resolution paths," *supra,* note 15; *see also* Symantec, Description of Trojan.Qhosts virus, http://www.symantec.com/security_response/writeup.jsp?docid=2003-100116-5901-99.

[18] Daniel Castro, "No, COICA Will Not Break the Internet," Innovation Policy blog, January 18, 2011, http://www.innovationpolicy.org/no-coica-will-not-break-the-internet.

likely have no idea that they are changing DNS servers. Those promoting pirate sites will simply create websites and postings that ask: "Frustrated by getting filtered when you try to watch movies? Click here to fix the problem." Long experience shows that high numbers of users will simply do just that; they will "click here" and thereby quickly circumvent the intended roadblock through automated processes such as DNS changers.

Would users care about performance? One theory states that users would avoid these non-U.S nameservers because they would be slower, if for no other reason that they are offshore and thus may take up to a substantial fraction of a second to return answers. There is some data that slower sites are slightly less popular, but it is unlikely that foreign DNS would slow things down enough, for a number of reasons.

First, the likely delay for a site would only be a few tenths of a second. Second, only the initial query to a domain is impacted. Third, most modern browsers implement something called DNS prefetching, performing the DNS lookup before the user even browses to a site. Consequently, users will likely not even experience the delay when navigating to a given site. Finally, from the perspective of a user seeking pirated content, a slightly slower site is much better than not being able to access the site and its infringing content at all.

However, even if one supposed that all malicious sites changing DNS settings were filtered, and even if one supposed that 100% of users leave their ISPs' DNS settings unchanged, mandatory DNS filtering still could be *trivially* evaded by individuals and even applications.

The IP number for the website of The Pirate Bay, a well-known peer-to-peer (P2P) organization that has often been connected to infringement allegations, is 194.71.107.15. Simply typing this number instead of www.piratebay.org into a browser's address line will take a user to the site. To avoid having to remember the number each time, PCs can easily be configured to bypass DNS filters.

Effectively, all systems have within them something called a hosts file, which is in text format. After simple editing of a hosts file with the additional line "www.thepiratebay.org 194.71.107.15", the DNS will no longer be consulted.

Many users will not have the expertise necessary to rewrite a host file. On the other hand, individuals who are skeptical of this potential for evasion should consider that software developers already are working on software to evade DNS filtration. A group calling itself "MafiaaFire" has developed a Firefox browser plugin that automatically redirects users requesting a seized domain to the desired site's new domain or server IP address.[19] (A screen image that shows the ease with which Internet users can implement such tools is in Appendix B). Infringers are almost certain to develop similar plugins that skip the DNS entirely, perhaps simply by putting links on their pages which offer to make necessary system changes with a click of the mouse.

This reality leads to one conclusion: PROTECT IP's DNS filtering *will* be evaded through trivial and often automated changes through easily accessible and installed software plugins. Given this

[19] http://mafiaafire.com/

strong potential for evasion, the long-term benefits of using mandated DNS filtering to combat infringement seem modest at best.

In addition, if the U.S. mandates and thereby legitimizes DNS filtering, more countries may impose their own flavor of DNS filtering. As this practice becomes more widespread, the extent to which a particular name is reachable will become a function of on which network and in which country a user sits, compromising the universality of DNS naming and thereby the "oneness" of the Internet. This situation will in turn increase the cost and challenge of developing new technologies, and reduce the reliability of the Internet as a whole. If the Internet moves towards a world in which every country is picking and choosing which domains to resolve and which to filter, the ability of American technology innovators to offer products and services around the world will decrease.

Moreover, circumvention poses risks to the security and stability of the DNS, which are explored in the following sections.

C. Circumvention Poses Performance and Security Risks

The likely circumvention techniques described above will expose users to new potential security threats. These security risks will not be limited to individuals. Banks, credit card issuers, health care providers, and others who have particular interests in security protections for data also will be affected. At the same time, a migration away from U.S.-based and ISP-provided DNS will harm U.S. network operators' ability to investigate and evaluate security threats. Intelligence and law enforcement officials who rely on high-quality network usage data afforded by centralized DNS resolution will face a similar reduction in the usefulness of DNS.[20]

1. Users Will Face Increased Cybersecurity Risk

As noted above, both users and operators of infringement sites will likely respond to DNS filtering by redirecting users' DNS settings to point outside of the United States. One cannot predict which DNS services they will use instead, but one can anticipate that some if not many of the new DNS resolvers will be well outside U.S. jurisdiction, possibly run by the same criminals running the infringement sites, and perhaps even on the same systems and hardware. This concern is not mere speculation: the use of non-U.S. DNS is already favored by malicious websites, viruses, and criminal gangs to evade U.S. law enforcement.

As a consequence of redirecting their DNS settings, users will face significantly increased security risks, as detailed below. Those risks, however, will not be obvious or well known to most users, and they will simply be unaware of the risks (and indeed, as noted above, the users may not even know that their DNS settings have been changed). Moreover, in households with shared computers, one user (say, a teenage music sharer) may redirect the DNS settings, but then those settings would carry over to when the parent later did online banking on the same computer. The teenager's redirection also could redirect banking information and put it in jeopardy. The effects of increased security vulnerability will be felt not just by users, but by U.S.

[20] A full discussion of the impact on law enforcement is outside the scope of this paper.

networks and businesses, including banks and credit card companies, which will internalize the costs of botnet disruptions, identity theft, and financial fraud.

Users on computers with redirected DNS settings will have a number of increased risks. First, operators of rogue DNS servers are less likely than major U.S. operators to support DNSSEC. Thus users who switch or are switched to such nameservers will not benefit from the security and trust DNSSEC is being implemented to provide. And the absence of support for DNSSEC may expose these users to greater risk from malicious nameserver operators.

Second, and critically, when traffic is pushed to potentially rogue servers, how will those servers handle the resolution of web and mail server lookups for military networks, U.S. banks, or social network sites used by U.S. citizens to communicate and share personal information and ideas? Circumvention has real consequences beyond evading the results of court-ordered filters. An infringement site that simply gains enough consent and cooperation from a user to shift his or her DNS resolution to the pirate site is not only insulated from the filters of PROTECT IP. The operator also gains access to *all* DNS traffic from that user:

> Every time the user seeks his bank, the pirate site has the opportunity to hijack it.
>
> Every time the user seeks an e-commerce site, the pirate site has the opportunity to impersonate it.
>
> Every email, every game, every Internet application that someone might use to be productive would potentially be exposed to manipulation.

Although some pirate operators may decide to run “honest” DNS servers in an effort to gain the trust of users, at least some of the overseas DNS servers are likely to act on their economic incentive to exploit their access to the sensitive communications of some Americans.

In the millions of DNS lookups exported from U.S. networks, many may prove innocuous, but some will fall in these sensitive categories, which will be attractive avenues for phishing and other cybercrime. In control of all of a user’s DNS traffic, a rogue resolver could easily return spurious results for sensitive queries. For example, a user could be sent an identical-looking but false and criminal website pretending to be Citibank.com, allowing the operator to gain access to and empty the user’s bank accounts.

If users of government or military networks violate sound security practices and redirect their DNS traffic to a non-U.S. DNS server, they could create national security risks given the sensitivity of those networks.[21] Redirection on such networks would risk providing non-U.S. networks a foothold in the DNS conversation, and the ability to monitor and manipulate resolution for potentially sensitive websites and mail servers, through denial-of-service attacks, disclosure attacks,[22] and an array of other avenues.

[21] Military information has been lost through P2P in the past; *See, e.g.,* Tim Wilson, “Army Hospital Breach May Be Result of P2P Leak,” *Dark Reading*, June 3, 2008, http://www.darkreading.com/taxonomy/index/oldarticleurl?articleID=211201106.

[22] “Disclosure attack” refers to the ability of an attacker to collect target intelligence information by analyzing client behavioral and query data.

2. *ISPs Will Lose Visibility into Network Security Threats*

DNS data currently provides ISPs an important and accurate picture of both traffic patterns and security threats on their network, which in turn is vital for both business planning and network protection. Data gleaned from their customers' access to their DNS servers can be useful for a number of purposes. First, it can allow an ISP to identify increases and shifts in traffic, which can inform infrastructure investment, network optimizations, interconnection strategies, and peering relationships. Even more critically, monitoring DNS data is a vital part of maintaining network security. By analyzing name lookups, ISPs are able to diagnose denial-of-service attacks, identify hosts that may be part of a botnet, and identify compromised domains serving as command-and-control servers or identify subscribers who may be at risk. These analyses in turn enable network administrators to combat these problems, both by addressing malicious traffic and by providing targeted assistance to the users of infected computers.

As users increasingly turn to other DNS servers to avoid the DNS filtering, ISPs have less and less ability to manage security threats and maintain effective network operations. By losing visibility into network security threats, ISPs will be less able to identify customer computers that have been infected by a virus and come under the control of a criminal botnet. At the same time that ISPs will be less able to identify infected computers, their security offices will be less able to assist law enforcement in investigating network security attacks or data loss and exfiltration.

The reduction of customer use of an enterprise, local network operator, or ISP's DNS service will mean that more compromised computers will go unidentified and uncorrected. Furthermore, the set of attributes that need to be evaluated when a customer calls an operator help desk for support will be much more extensive, and will increase both cost and debugging complexity.

3. *CDNs Would Likely Face Degraded Performance*

Routing DNS traffic to offshore servers will also affect network performance within the United States, and will increase costs for ISPs. For DNS queries themselves, any delay will be minimal. However, for content delivered from Content Distribution Networks (CDNs) the impact will be more severe.

CDNs localize content delivery by distributing the same content across a number of servers on a wide range of networks. This localization reduces network congestion and decreases the load that would otherwise be put on a single server. Many CDNs use the IP address of the DNS resolver to estimate a user's location and route the user to the fastest available server. To such networks, U.S. users who have changed their DNS resolvers for all lookups will appear to the CDNs to be browsing from abroad. As a result, these users could be routed to offshore servers not just for DNS queries, but also for content, undermining precisely the benefits CDNs provide by optimizing traffic distribution to account for proximity of client and server.

Inefficient server selection would cause small delays for users, but high costs for commercial actors who must pay higher costs of latency and added network resources in order to provide the same level of service. The higher costs will negatively impact the business of both the providers of high-value, high-bandwidth (and non-infringing) content that overwhelmingly make up the customer base of CDNs, as well as the CDN operators themselves. To the extent that poor server selection results in increased traffic over international links, as is likely, it will also increase the traffic load and network congestion experienced by a wider range of network operators.

D. DNS Interdependencies Will Lead to Collateral Damage

Two likely situations ways can be identified in which DNS filtering could lead to non-targeted and perfectly innocent domains being filtered. The likelihood of such collateral damage means that mandatory DNS filtering could have far more than the desired effects, affecting the stability of large portions of the DNS.

First, it is common for different services offered by a domain to themselves have names in some other domain, so that example.com's DNS service might be provided by isp.net and its e-mail service might be provided by asp.info. This means that variation in the meaning or accessibility of asp.info or isp.net could indirectly but quite powerfully affect the usefulness of example.com. If a legitimate site points to a filtered domain for its authoritative DNS server, lookups from filtering nameservers for the legitimate domain will also fail. These dependencies are unpredictable and fluid, and extremely difficult to enumerate. When evaluating a targeted domain, it will not be apparent what other domains might point to it in their DNS records.

In addition, one IP address may support multiple domain names and websites; this practice is called "virtual hosting" and is very common. Under PROTECT IP, implementation choices are (properly) left up to DNS server operators, but unintended consequences will inevitably result. If an operator or filters the DNS traffic to and from one IP address or host, it will bring down all of the websites supported by that IP number or host. The bottom line is that the filtering of one domain name or hostname can pull down unrelated sites down across the globe.

Second, some domain names use "subdomains" to identify specific customers. For example, blogspot.com uses subdomains to support its thousands of users; blogspot.com may have customers named Larry and Sergey whose blog services are at larry.blogspot.com and sergey.blogspot.com. If Larry is an e-criminal and the subject of an action under PROTECT IP, it is possible that blogspot.com could be filtered, in which case Sergey would also be affected, although he may well have had no knowledge of Larry's misdealings. This type of collateral damage was demonstrated vividly by the ICE seizure of mooo.com, in which over 84,000 subdomains were mistakenly filtered.[23]

The authors of the paper understand that sites offering such subdomain hosting are not the target of PROTECT IP, but the possibility for such unintended filtering remains. Despite sharing a parent domain, subdomains, as well as their content, often have little or nothing to do with one another. The existence of additional subdomains may not be readily apparent upon reviewing whatever content is served at a particular subdomain, just as visiting google.com gives no indication of the existence of yahoo.com, despite the fact that the two domains share the .com top-level domain. Thus it is possible for an examination of one subdomain to conclude without ever revealing the existence of others that would be affected by a filtering order instituted in the DNS.

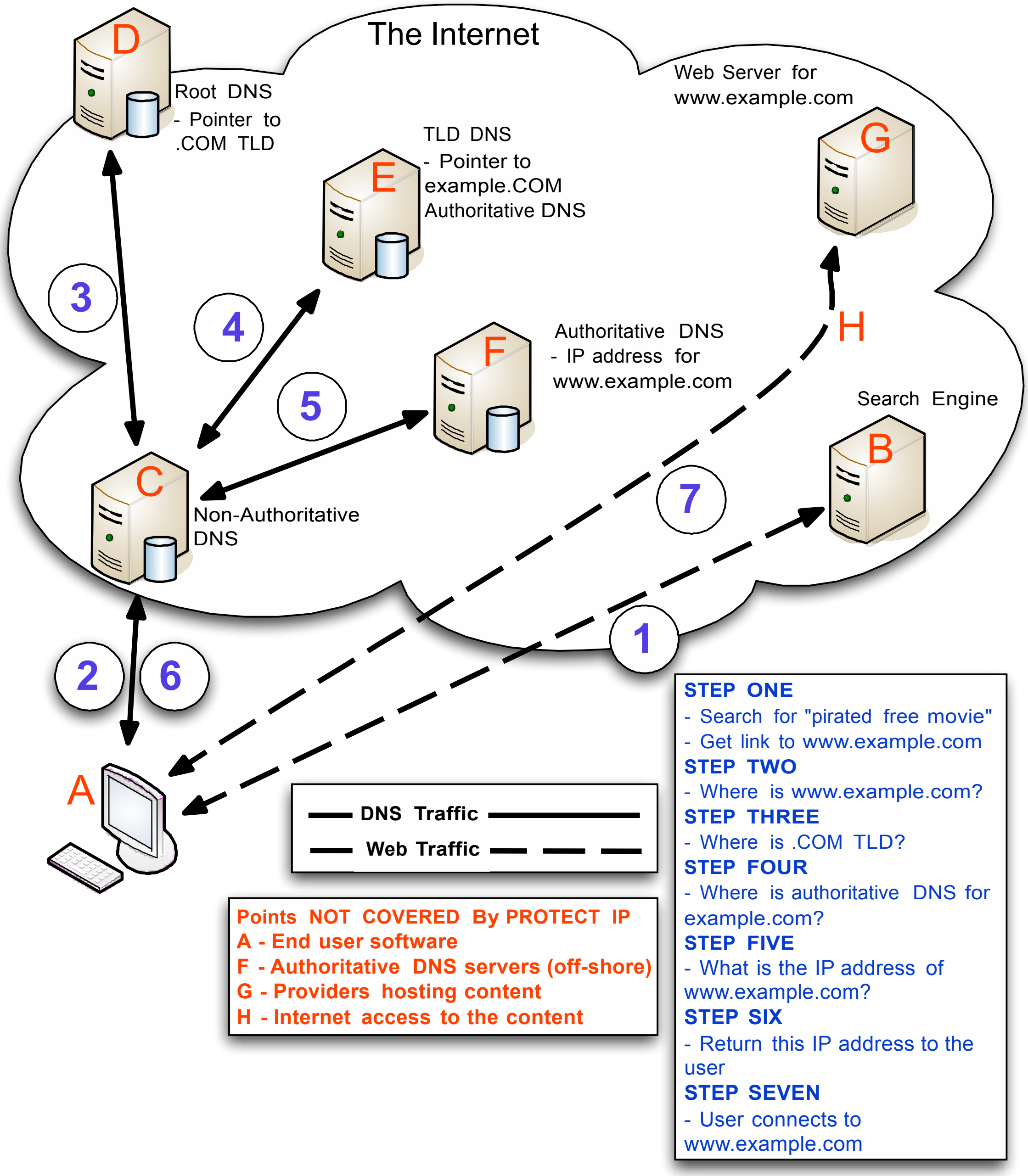
[23] Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *InformationWeek*, February 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/229218959.

IV. Conclusion

As stated above, we strongly believe that the goals of PROTECT IP are compelling, and that intellectual property laws should be enforced against those who violate them. But as discussed in this paper, the mandated DNS filtering provisions found in the PROTECT IP Act raise very serious security and technical concerns. We believe that the goals of PROTECT IP can be accomplished without reducing DNS security and stability, through strategies such as better international cooperation on prosecutions and the other remedies contained in PROTECT IP other than DNS-related provisions. We urge Congress to reject the DNS filtering portions of the Act.

APPENDIX A

The figure below may be helpful in understanding the DNS filtering method specified in PROTECT IP



Points NOT COVERED By PROTECT IP
A - End user software
F - Authoritative DNS servers (off-shore)
G - Providers hosting content
H - Internet access to the content

STEP ONE
- Search for "pirated free movie"
- Get link to www.example.com

STEP TWO
- Where is www.example.com?

STEP THREE
- Where is .COM TLD?

STEP FOUR
- Where is authoritative DNS for example.com?

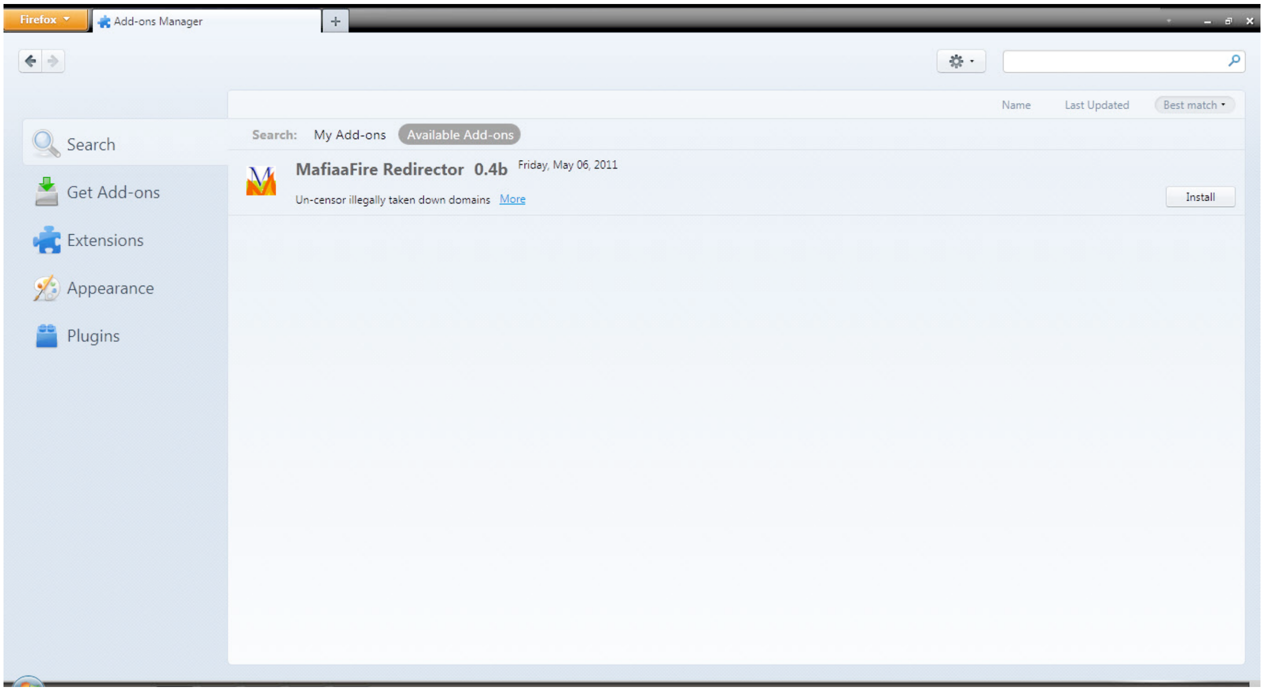
STEP FIVE
- What is the IP address of www.example.com?

STEP SIX
- Return this IP address to the user

STEP SEVEN
- User connects to www.example.com

APPENDIX B

Some browser plugins are easily installed, and would allow users to avoid the DNS filtering contemplated by PROTECT-IP. The MafiaaFire redirector, shown below, was created in direct response to domain-seizures and the introduction of COICA in 2010.



MafiaaFire Redirector 0.4b Friday, May 06, 2011

Un-censor illegally taken down domains More

Screen-captured on 05/25/11 at 10:45 a.m.

ABOUT THE AUTHORS

Steve Crocker is CEO of Shinkuro, Inc., a security-oriented consulting and development company, and has been leading Shinkuro's work on deployment of DNSSEC, the security extension to DNS. He currently serves as vice chair of the board of ICANN and served as chair of ICANN's Security and Stability Advisory Committee from its inception in 2002 until 2010. He has been active in the Internet community since 1968 when he helped define the original set of protocols for the Arpanet, founded the RFC series of publications and organized the Network Working Group, the forerunner of today's Internet Engineering Task Force (IETF). He later served as the first Area Director for Security in the IETF. Over his forty-plus years in network research, development, and management, he has been an R&D Program Manager at DARPA, senior researcher at University of Southern California's Information Sciences Institute, Director of Aerospace Corp's Computer Science Laboratory, vice president of Trusted Information Systems, co-founder, senior vice president and CTO of CyberCash, Inc. and co-founder and CEO of Longitude Systems, Inc.

David Dagon is a post-doctoral researcher at Georgia Institute of Technology studying DNS security and the malicious use of the domain resolution system. He is a co-founder of Damballa, an Internet security company providing DNS-based defense technologies. He has authored numerous peer- reviewed studies of DNS security, created patent-pending DNS security technologies, and proposed anti-poisoning protocol changes to DNS.

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and Microsoft. Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases. Dan is best known for his work finding a critical flaw in the Internet's Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet's infrastructure of all time. Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative. Dan is presently developing systems to reduce the cost and complexity of securing critical infrastructure.

Danny McPherson is Chief Security Officer for Verisign, Inc., where he is responsible for strategic direction, research, and innovation in infrastructure, and information security. He currently serves on the Internet Architecture Board (IAB), ICANN's Security and Stability Advisory Council, the FCC's Network Reliability and Interoperability Council (NRIC), and several other industry forums. He has been active within the Internet operations, security, research, and standards communities for nearly 20 years, and has authored a number of books and other publications related to these topics. Previously, he was CSO of Arbor Networks, and prior to that held technical leadership positions with Amber Networks, Qwest Communications, Genuity, MCI Communications, and the U.S. Army Signal Corp.

Paul Vixie founded Internet Systems Consortium in 1996 and served as ISC's President from 1996 to 2011 when he was named Chairman and Chief Scientist. Vixie was the principal author of BIND versions 4.9 to 8.2, which is the leading DNS server software in use today. He was also a principal author of RFC 1996 (DNS NOTIFY), RFC 2136 (DNS UPDATE), and RFC 2671 (EDNS), coauthor of RFC 1876 (DNS LOC), RFC 2317 (DNS for CIDR), and RFC 2845 (DNS TSIG). Vixie's other interests are Internet governance and policy, and distributed system security.

The New York Times

Internet Piracy and How to Stop It

June 8, 2011

Online piracy is a huge business. A recent study found that Web sites offering pirated digital content or counterfeit goods, like illicit movie downloads or bootleg software, record 53 billion hits per year. That robs the industries that create and sell intellectual products of hundreds of billions of dollars.

The problem is particularly hard to crack because the villains are often in faraway countries. Bad apples can be difficult to pin down in the sea of Web sites, and pirates can evade countervailing measures as easily as tweaking the name of a Web site.

Commendably, the Senate Judiciary Committee is trying to bolster the government's power to enforce intellectual property protections. Last month, the committee approved the Protect IP Act, which creates new tools to disrupt illegal online commerce.

The bill is not perfect. Its definition of wrongdoing is broad and could be abused by companies seeking to use the law to quickly hinder Web sites. Some proposed remedies could also unintentionally reduce the safety of the Internet. Senator Ron Wyden put a hold on the bill over these issues, which, he argued, could infringe on the right to free speech. The legislation is, therefore, in limbo, but it should be fixed, not discarded.

The bill defines infringing Web sites as those that have "no significant use other than engaging in, enabling, or facilitating" the illegal copying or distribution of copyrighted material in "substantially complete form" — entire movies or songs, not just snippets.

If the offender can't be found to answer the accusation (a likely occurrence given that most Web sites targeted will be overseas), the government or a private party can seek an injunction from a judge to compel advertising networks and payment systems like MasterCard or PayPal to stop doing business with the site.

The government — but not private parties — can use the injunction to compel Internet service providers to redirect traffic by not translating a Web address into the numerical language that computers understand. And they could force search engines to stop linking to them.

The broadness of the definition is particularly worrisome because private companies are given a right to take action under the bill. In one notorious case, a record label demanded that YouTube take down a home video of a toddler jiggling in the kitchen to a tune by Prince, claiming it violated copyright law. Allowing firms to go after a Web site that "facilitates" intellectual property theft might encourage that kind of overreaching — and allow the government to black out a site.

Some of the remedies are problematic. A group of Internet safety experts cautioned that the procedure to redirect Internet traffic from offending Web sites would mimic what hackers do when they take over a domain. If it occurred on a large enough scale it could impair efforts to enhance the safety of the domain name system.

This kind of blocking is unlikely to be very effective. Users could reach offending Web sites simply by writing the numerical I.P. address in the navigator box, rather than the URL. The Web sites could distribute free plug-ins to translate addresses into numbers automatically.

The bill before the Senate is an important step toward making piracy less profitable. But it shouldn't pass as is. If protecting intellectual property is important, so is protecting the Internet from overzealous enforcement.

Los Angeles Times

Editorial: Policing the Internet

A Senate bill aims to cut off support for any site found by the courts to be 'dedicated' to copyright or trademark infringement. Its goals are laudable, but its details are problematic.

June 7, 2011

Hollywood studios, record labels and other U.S. copyright and trademark owners are pushing Congress to give them more protection against parasitical foreign websites that are profiting from counterfeit or bootlegged goods. The Senate Judiciary Committee has responded with a bill (S 968) that would force online advertising networks, credit card companies and search engines to cut off support for any site found by the courts to be "dedicated" to copyright or trademark infringement. Its goals are laudable, but its details are problematic.

The global nature of the Internet has spawned a profusion of websites in countries that can't or won't enforce intellectual property law. Under S 968, if a website were deemed by a court to be dedicated to infringing activities, federal agents could then tell the U.S. companies that direct traffic, process payments, serve advertisements and locate information online to end their support for the site in question. Copyright and trademark owners would be able to follow up those court orders by seeking injunctions against payment processors and advertising networks that do not comply.

Cutting off the financial lifeblood of companies dedicated to piracy and counterfeiting makes sense. A similar approach to illegal online gambling has shown that it is technically feasible for payment processors to stop directing dollars from U.S. bettors to gambling sites anywhere in the world. The operators of the largest online advertising networks say they can do the same, although they object to the bill's proposal to let copyright and trademark owners seek injunctions against them.

The main problem with the bill is in its effort to render sites invisible as well as unprofitable. Once a court determines that a site is dedicated to infringing, the measure would require the companies that operate domain-name servers to steer Internet users away from it. This misdirection, however, wouldn't stop people from going to the site, because it would still be accessible via its underlying numerical address or through overseas domain-name servers.

A group of leading Internet engineers has warned that the bill's attempt to hide piracy-oriented sites could hurt some legitimate sites because of the way domain names can be shared or have unpredictable mutual dependencies. And by encouraging Web consumers to use foreign or underground servers, the measure could undermine efforts to create a more reliable and fraud-resistant domain-name system. These risks argue for Congress to take a more measured approach to the problem of overseas rogue sites.

OregonLive.com

Stop The Internet Blacklist Bill
August 28, 2011
By David Segal and Patrick Ruffini

We are Tea Partiers and bleeding-heart liberals, we are artists and investment bankers, we represent the left and the right, and we support Senator Wyden as he comes forward, yet again, as a stalwart champion for First Amendment rights, innovation and digital security.

The problem at hand is a bill called the "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act" (PROTECT IP) and it aims to permanently change our digital landscape – that's why we're calling it what it is: The Internet Blacklist Bill.

Imagine you're the successful owner of a heavily trafficked website. Your income and that of those with whom you work depends entirely on the advertising revenue and payments provided by visitors to your site. One day, without warning, your site no longer appears at its domain, your advertisers have backed out, and you can't even find your site on Google. You've been disappeared – blacklisted by new regulations set by Congress in the PROTECT IP Act.

If passed, PROTECT IP would give the government dramatic new powers to target websites dedicated to the illegal distribution of copyrighted content. Violating sites would have their domain disabled in DNS servers (the servers that match the domain name with the numerical IP address and make sure you go to the websites you want to), and all third party sites, including search engines, would be required to remove the site from their registries and disable all links to the domain in question.

Even worse, PROTECT IP also includes a "private right of action" that would allow rights holders to obtain a temporary restraining order against a domain in civil court. Instead, big content providers like the RIAA can target websites at their whim, urging courts to shut down anyone they accuse of violating U.S. copyright law.

The entities accused of infringement wouldn't even get their day in court until after they've been shut down – they could appeal to the courts for relief only after the fact.

Big interest groups in favor of PROTECT IP have recently pushed the idea that to be against this bill is to handicap aspiring artists and to be in opposition to a fair marketplace. We vehemently disagree. Regulations stipulated in PROTECT IP would cause tremendous damage to the infrastructure and security of the Internet and ultimately undermine the millions of entrepreneurs, businesses and artists who depend on a free, uninterrupted communications platform.

Already, venture capitalists, engineers, and entrepreneurs (including Google CEO Eric Schmidt) have penned letters and petitions against PROTECT IP, citing the corrosive effect it would have on digital security and innovation. Human rights activists are terrified that PROTECT IP will provide comfort to totalitarian regimes that seek ever more control over Internet users in their own countries. More that 400,000 Americans have urged their lawmakers to oppose the bill. But ultimately, we are depending on lawmakers, like Sen. Wyden to make the final decisions and defend our rights.

David Segal is Executive Director of the left-leaning Demand Progress and Patrick Ruffini is Executive Director of the right-leaning Don't Censor the Net, which together have generated more than 400,000 anti-PIPA contacts to Congress.