AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

STOP ONLINE PIRACY ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

ON

H.R. 3261

NOVEMBER 16, 2011

Serial No. 112–154

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

71–240 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
[Vacant]

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

CONTENTS

NOVEMBER 16, 2011

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

STOP ONLINE PIRACY ACT

WEDNESDAY, NOVEMBER 16, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to call, at 10:06 a.m., in room 2141, Rayburn Office Building, the Honorable Lamar Smith (Chairman of the Committee) presiding.

Present: Representatives Smith, Coble, Goodlatte, Lungren, Chabot, Issa, Forbes, King, Franks, Gohmert, Jordan, Poe, Chaffetz, Griffin, Marino, Gowdy, Ross, Adams, Quayle, Amodei, Conyers, Berman, Nadler, Watt, Lofgren, Jackson Lee, Waters, Cohen, Johnson, Quigley, Chu, Deutch, and Sánchez.

Staff present: (Majority) David Whitney, Counsel; Olivia Lee, Clerk; and (Minority) Jason Everett, Counsel.

Mr. SMITH. Good morning. The Judiciary Committee will come to order. Without objection, the Chair is authorized to declare recesses of the Committee at any time.

I am going to recognize myself for an opening statement, then the Ranking Member, and then the Chairman and the Ranking Member of the appropriate Subcommittee.

Today's hearing is on legislation that will help protect one of the most productive sectors of the American economy. While the Digital Millennium Copyright Act does provide some relief to copyright owners whose works are infringed, it only helps in limited circumstances. The DMCA provides no effective relief when a rogue website is foreign-based and foreign operated, like The Pirate Bay, the 89th most visited site in the U.S. It does not protect trademark owners and consumers from counterfeit and unsafe products, like fake prescription medicines and misbranded branded drugs that are often presented to the public by unlicensed online pharmacies. Nor does the law assist copyright owners when rogue websites contribute to the theft of intellectual property on a massive scale.

And, finally, this does nothing to address the use of certain intermediaries, such as payment processors and Internet advertising services, that are used by criminals to fund the illegal activities.

Mr. SCOTT. Mr. Chairman, I am having trouble hearing your statement.

Mr. SMITH. I would not want anyone to miss my statement, so I will make sure that the sound system is working and that I am close enough to the mic.

Mr. SCOTT. Turn his mic way up.

Mr. SMITH. That is where the Stop Online Piracy Act comes in. This bill focuses not on technology, but on preventing those who engage in criminal behavior from reaching directly into the U.S. market to harm American consumers. We cannot continue a system that allows criminals to disregard our laws and import counterfeit and pirated goods across our physical borders, nor can we fail to take effective and meaningful action when criminals misuse the Internet.

The problem of rogue websites is real, immediate, and wide spread. It harms all sectors of the economy, and its scope is staggering. One recent survey found that nearly one-quarter of global Internet traffic infringes on copyrights. A second study found that 43 sites classified as digital piracy, generated 53 billion visits per year, and that 26 sites selling just counterfeit prescription drugs generated 51 million hits annually.

Since the United States produces the most intellectual property, our country has the most to lose if we fail to address the problem of these rogue websites. Responsible companies and public officials have taken note of the corrosive and damaging effects of rogue websites. One of our witnesses today represents MasterCard Worldwide, a company that takes seriously its obligation to reduce the amount of stolen intellectual property on the Internet. MasterCard deserves thanks for its commitment to support legislation that addresses the problems of online piracy.

In contrast, another one of the companies represented here today has sought to obstruct the Committee's consideration of bipartisan legislation. Perhaps this should come as no surprise, given that Google just settled a Federal criminal investigation into the company's active promotion of a rogue websites that pushed illegal prescription and counterfeit drugs on American consumers. In announcing a half billion dollar forfeiture of illegal profit, the U.S. Attorney, Peter Neronha, who led the investigation, stated, "Suffice it to say that this is not two or three rogue employees of the consumer service level doing this. This was a corporate decision to engage in this conduct."

Over several years, Google ignored repeated warnings from the National Association of Boards of Pharmacy and the National Center on Addiction and Substance Abuse at Columbia University, that the company was violating Federal law. The company also disregarded requests to block advertisements from rogue pharmacies, screen such sites from searches, and provide warnings about buying drugs over the Internet.

The Wall Street Journal reports Mr. Neronha characterized Google's efforts to appear to control unlawful advertisements as window dressing since "It allowed Google to continue earning revenues from the allegedly illicit ad sales, even as it professed to be taking action against them." Given Google's record, their objection to authorizing a court to order a search engine to not steer consumers to foreign rogue sites is easily understood.

Unfortunately, the theft of America's intellectual property costs the United States economy more than $100 billion annually and results in a loss of thousands of American jobs. Under current law, rogue sites that profit from selling pirated goods are often out of the reach of U.S. law enforcement agencies and operate without

consequences. The Stop Online Piracy Act helps stop flow of revenues to rogue websites and insurers. The profits from American innovations go to American innovators.

Protecting America's intellectual property will help our economy, create jobs, and discourage illegal websites.

That concludes my opening statement, and the gentleman from Michigan, the Ranking Member of the Judiciary Committee, is recognized for his opening statement.

[The text of the bill, H.R. 3261, follows:]

I

112TH CONGRESS
1ST SESSION

H. R. 3261

To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 26, 2011

Mr. SMITH of Texas (for himself and Mr. CONYERS, Mr. GOODLATTE, Mr. BERMAN, Mr. GRIFFIN of Arkansas, Mr. GALLEGLY, Mr. DEUTCH, Mr. CHABOT, Mr. ROSS of Florida, Mrs. BLACKBURN, Mrs. BONO MACK, Mr. TERRY, and Mr. SCHIFF) introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Stop Online Piracy Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. SAVINGS AND SEVERABILITY CLAUSES.

(a) SAVINGS CLAUSES.—

(1) FIRST AMENDMENT.—Nothing in this Act shall be construed to impose a prior restraint on free speech or the press protected under the 1st Amendment to the Constitution.

(2) TITLE 17 LIABILITY.—Nothing in title I shall be construed to enlarge or diminish liability, including vicarious or contributory liability, for any cause of action available under title 17, United States Code, including any limitations on liability under such title.

(b) SEVERABILITY.—If any provision of this Act, or the application of the provision to any person or circumstance, is held to be unconstitutional, the other provisions or the application of the provision to other persons or circumstances shall not be affected thereby.

TITLE I—COMBATING ONLINE PIRACY

SEC. 101. DEFINITIONS.

In this title:

(1) DOMAIN NAME.—The term "domain name" has the meaning given that term in section 45 of the Lanham Act (15 U.S.C. 1127) and includes any subdomain designation using such domain name as part of an electronic address on the Internet to identify a unique online location.

(2) DOMAIN NAME SYSTEM SERVER.—The term "domain name system server" means a server or other mechanism used to provide the Internet protocol address associated with a domain name.

(3) DOMESTIC DOMAIN NAME.—The term "domestic domain name" means a domain name that is registered or assigned by a domain name registrar, domain name registry, or other domain name registration authority, that is located within a judicial district of the United States.

(4) DOMESTIC INTERNET PROTOCOL ADDRESS.—The term "domestic Internet Protocol address" means an Internet Protocol address for which the corresponding Internet Protocol allocation entity is located within a judicial district of the United States.

(5) DOMESTIC INTERNET SITE.—The term "domestic Internet site" means an Internet site for which the corresponding domain name or, if there is no domain name, the corresponding Internet Protocol address, is a domestic domain name or domestic Internet Protocol address.

(6) FOREIGN DOMAIN NAME.—The term "foreign domain name" means a domain name that is not a domestic domain name.

(7) FOREIGN INTERNET PROTOCOL ADDRESS.—The term "foreign Internet Protocol address" means an Internet Protocol address that is not a domestic Internet protocol address.

(8) FOREIGN INTERNET SITE.—The term "foreign Internet site" means an Internet site that is not a domestic Internet site.

(9) INCLUDING.—The term "including" means including, but not limited to.

(10) INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR.—The term "Intellectual Property Enforcement Coordinator" means the Intellectual Property Enforcement Coordinator appointed under section 301 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (15 U.S.C. 8111).

(11) INTERNET.—The term "Internet" has the meaning given that term in section 5362(5) of title 31, United States Code.

(12) INTERNET ADVERTISING SERVICE.—The term "Internet advertising service" means a service that for compensation sells, purchases, brokers, serves, inserts, verifies, clears, or otherwise facilitates the placement of an advertisement, including a paid or sponsored search result, link, or placement, that is rendered in viewable form for any period of time on an Internet site.

(13) INTERNET PROTOCOL.—The term "Internet Protocol" means a protocol used for communicating data across a packet-switched internetwork using the Transmission Control Protocol/Internet Protocol, and includes any predecessor or successor protocol to such protocol.

(14) INTERNET PROTOCOL ADDRESS.—The term "Internet Protocol address" means a numerical label that is assigned to each device that participates in a computer network that uses the Internet Protocol for communication.

(15) INTERNET PROTOCOL ALLOCATION ENTITY.—The term "Internet Protocol allocation entity" means, with respect to a particular Internet Protocol address, the entity, local internet registry, or regional internet registry to which the smallest applicable block of Internet Protocol addresses containing that address is allocated or assigned by a local internet registry, regional internet registry, or other Internet Protocol address allocation authority, according to the applicable publicly available database of allocations and assignments, if any.

(16) INTERNET SEARCH ENGINE.—The term "Internet search engine" means a service made available via the Internet that searches, crawls, categorizes, or indexes information or Web sites available elsewhere on the Internet and on the basis of a user query or selection that consists of terms, concepts, categories, questions, or other data returns to the user a means, such as a hyperlinked list of Uniform Resource Locators, of locating, viewing, or downloading such information or data available on the Internet relating to such query or selection.

(17) INTERNET SITE.—The term "Internet site" means the collection of digital assets, including links, indexes, or pointers to digital assets, accessible through the Internet that are addressed relative to a common domain name or, if there is no domain name, a common Internet Protocol address.

(18) LANHAM ACT.—The term "Lanham Act" means the Act entitled "An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes", approved July 5, 1946 (commonly referred to as the "Trademark Act of 1946" or the "Lanham Act").

(19) NONAUTHORITATIVE DOMAIN NAME SERVER.—The term "nonauthoritative domain name server" means a server that does not contain complete copies of domains but uses a cache file that is comprised of previous domain name server lookups, for which the server has received an authoritative response in the past.

(20) OWNER; OPERATOR.—The terms "owner" or "operator", when used in connection with an Internet site, includes, respectively, any owner of a majority interest in, or any person with authority to operate, such Internet site.

(21) PAYMENT NETWORK PROVIDER.—

(A) IN GENERAL.—The term "payment network provider" means an entity that directly or indirectly provides the proprietary services, infrastructure, and software to effect or facilitate a debit, credit, or other payment transaction.

(B) RULE OF CONSTRUCTION.—For purposes of this paragraph, a depository institution (as such term is defined under section 3 of the Federal Deposit Insurance Act) or credit union that initiates a payment transaction shall not be construed to be a payment network provider based solely on the offering or provision of such service.

(22) SERVICE PROVIDER.—The term "service provider" means a service provider as defined in section 512(k)(1) of title 17, United States Code, that operates a nonauthoritative domain name system server.

(23) U.S.-DIRECTED SITE.—The term "U.S.-directed site" means an Internet site or portion thereof that is used to conduct business directed to residents of the United States, or that otherwise demonstrates the existence of minimum contacts sufficient for the exercise of personal jurisdiction over the owner or operator of the Internet site consistent with the Constitution of the United States, based on relevant evidence that may include whether—

(A) the Internet site is used to provide goods or services to users located in the United States;

(B) there is evidence that the Internet site or portion thereof is intended to offer or provide—

(i) such goods and services,

(ii) access to such goods and services, or

(iii) delivery of such goods and services,

to users located in the United States;

(C) the Internet site or portion thereof does not contain reasonable measures to prevent such goods and services from being obtained in or delivered to the United States; and

(D) any prices for goods and services are indicated or billed in the currency of the United States.

(24) UNITED STATES.—The term "United States" includes any commonwealth, possession, or territory of the United States.

SEC. 102. ACTION BY ATTORNEY GENERAL TO PROTECT U.S. CUSTOMERS AND PREVENT U.S. SUPPORT OF FOREIGN INFRINGING SITES.

(a) DEFINITION.—For purposes of this section, a foreign Internet site or portion thereof is a "foreign infringing site" if—

(1) the Internet site or portion thereof is a U.S.-directed site and is used by users in the United States;

(2) the owner or operator of such Internet site is committing or facilitating the commission of criminal violations punishable under section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of title 18, United States Code; and

(3) the Internet site would, by reason of acts described in paragraph (1), be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site.

(b) ACTION BY THE ATTORNEY GENERAL.—

(1) IN PERSONAM.—The Attorney General may commence an in personam action against—

(A) a registrant of a domain name used by a foreign infringing site; or

(B) an owner or operator of a foreign infringing site.

(2) IN REM.—If through due diligence the Attorney General is unable to find a person described in subparagraph (A) or (B) of paragraph (1), or no such person found has an address within a judicial district of the United States, the Attorney General may commence an in rem action against a foreign infringing site or the foreign domain name used by such site.

(3) NOTICE.—Upon commencing an action under this subsection, the Attorney General shall send a notice of the alleged violation and intent to proceed under this section—

(A) to the registrant of the domain name of the Internet site—

(i) at the postal and electronic mail addresses appearing in the applicable publicly accessible database of registrations, if any, and to the extent such addresses are reasonably available; and

(ii) via the postal and electronic mail addresses of the registrar, registry, or other domain name registration authority that registered or assigned the domain name of the Internet site, to the extent such addresses are reasonably available; or

(B) to the owner or operator of the Internet site—

(i) at the primary postal and electronic mail addresses for such owner or operator that is provided on the Internet site, if any, and to the extent such addresses are reasonably available; or

(ii) if there is no domain name of the Internet site, via the postal and electronic mail addresses of the Internet Protocol allocation entity appearing in the applicable publicly accessible database of allocations and assignments, if any, and to the extent such addresses are reasonably available; or

(C) in any other such form as the court may provide, including as may be required by rule 4(f) of the Federal Rules of Civil Procedure.

(4) SERVICE OF PROCESS.—For purposes of this section, the actions described in this subsection shall constitute service of process.

(5) RELIEF.—On application of the Attorney General following the commencement of an action under this section, the court may issue a temporary restraining order, a preliminary injunction, or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure, against a registrant of a domain name used by the foreign infringing site or an owner or operator of the foreign infringing site or, in an action brought in rem under paragraph (2), against the foreign infringing site or a portion of such site, or the domain name used by such site, to cease and desist from undertaking any further activity as a foreign infringing site.

(c) ACTIONS BASED ON COURT ORDERS.—

(1) SERVICE.—A process server on behalf of the Attorney General, with prior approval of the court, may serve a copy of a court order issued pursuant to this section on similarly situated entities within each class described in paragraph (2). Proof of service shall be filed with the court.

(2) REASONABLE MEASURES.—After being served with a copy of an order pursuant to this subsection, the following shall apply:

(A) SERVICE PROVIDERS.—

(i) IN GENERAL.—A service provider shall take technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site (or portion thereof) that is subject to the order, including measures designed to prevent the domain name of the foreign infringing site (or portion

thereof) from resolving to that domain name's Internet Protocol address. Such actions shall be taken as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order.

(ii) LIMITATIONS.—A service provider shall not be required—

(I) other than as directed under this subparagraph, to modify its network, software, systems, or facilities;

(II) to take any measures with respect to domain name resolutions not performed by its own domain name server; or

(III) to continue to prevent access to a domain name to which access has been effectively disabled by other means.

(iii) CONSTRUCTION.—Nothing in this subparagraph shall affect the limitation on the liability of a service provider under section 512 of title 17, United States Code.

(iv) TEXT OF NOTICE.—The Attorney General shall prescribe the text of any notice displayed to users or customers of a service provider taking actions pursuant to this subparagraph. Such text shall state that an action is being taken pursuant to a court order obtained by the Attorney General.

(B) INTERNET SEARCH ENGINES.—A provider of an Internet search engine shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to prevent the foreign infringing site that is subject to the order, or a portion of such site specified in the order, from being served as a direct hypertext link.

(C) PAYMENT NETWORK PROVIDERS.—

(i) PREVENTING AFFILIATION.—A payment network provider shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States or subject to the jurisdiction of the United States and the payment account—

(I) which is used by the foreign infringing site, or portion thereof, that is subject to the order; and

(II) through which the payment network provider would complete such payment transactions.

(ii) NO DUTY TO MONITOR.—A payment network provider shall be considered to be in compliance with clause (i) if it takes action described in that clause with respect to accounts it has as of the date on which a copy of the order is served, or as of the date on which the order is amended under subsection (e).

(D) INTERNET ADVERTISING SERVICES.—

(i) REQUIRED ACTIONS.—An Internet advertising service that contracts to provide advertising to or for the foreign infringing site, or portion thereof, that is subject to the order, or that knowingly serves advertising to or for such site or such portion thereof, shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to—

(I) prevent its service from providing advertisements to or relating to the foreign infringing site that is subject to the order or a portion of such site specified in the order;

(II) cease making available advertisements for the foreign infringing site or such portion thereof, or paid or sponsored search results, links, or other placements that provide access to such foreign infringing site or such portion thereof; and

(III) cease providing or receiving any compensation for advertising or related services to, from, or in connection with such foreign infringing site or such portion thereof.

(ii) NO DUTY TO MONITOR.—An internet advertising service shall be considered to be in compliance with clause (i) if it takes action described in that clause with respect to accounts it has as of the date on which a copy of the order is served, or as of the date on which the order is amended under subsection (e).

(3) COMMUNICATION WITH USERS.—Except as provided under paragraph (2)(A)(iv), an entity taking an action described in this subsection shall determine the means to communicate such action to the entity's users or customers.

(4) ENFORCEMENT OF ORDERS.—

(A) IN GENERAL.—To ensure compliance with orders issued pursuant to this section, the Attorney General may bring an action for injunctive relief—

(i) against any entity served under paragraph (1) that knowingly and willfully fails to comply with the requirements of this subsection to compel such entity to comply with such requirements; or

(ii) against any entity that knowingly and willfully provides or offers to provide a product or service designed or marketed for the circumvention or bypassing of measures described in paragraph (2) and taken in response to a court order issued pursuant to this subsection, to enjoin such entity from interfering with the order by continuing to provide or offer to provide such product or service.

(B) RULE OF CONSTRUCTION.—The authority granted the Attorney General under subparagraph (A)(i) shall be the sole legal remedy to enforce the obligations under this section of any entity described in paragraph (2).

(C) DEFENSE.—A defendant in an action under subparagraph (A)(i) may establish an affirmative defense by showing that the defendant does not have the technical means to comply with this subsection without incurring an unreasonable economic burden, or that the order is not authorized by this subsection. Such showing shall not be presumed to be a complete defense but shall serve as a defense only for those measures for which a technical limitation on compliance is demonstrated or for such portions of the order as are demonstrated to be unauthorized by this subsection.

(D) DEFINITION.—For purposes of this paragraph, a product or service designed or marketed for the circumvention or bypassing of measures described in paragraph (2) and taken in response to a court order issued pursuant to this subsection includes a product or service that is designed or marketed to enable a domain name described in such an order—

(i) to resolve to that domain name's Internet protocol address notwithstanding the measures taken by a service provider under paragraph (2) to prevent such resolution; or

(ii) to resolve to a different domain name or Internet Protocol address that the provider of the product or service knows, reasonably should know, or reasonably believes is used by an Internet site offering substantially similar infringing activities as those with which the infringing foreign site, or portion thereof, subject to a court order under this section was associated.

(5) IMMUNITY.—

(A) IMMUNITY FROM SUIT.—Other than in an action pursuant to paragraph (4), no cause of action shall lie in any Federal or State court or administrative agency against any entity served with a copy of a court order issued under this subsection, or against any director, officer, employee, or agent thereof, for any act reasonably designed to comply with this subsection or reasonably arising from such order.

(B) IMMUNITY FROM LIABILITY.—Other than in an action pursuant to paragraph (4)—

(i) any entity served with a copy of an order under this subsection, and any director, officer, employee, or agent thereof, shall not be liable for any act reasonably designed to comply with this subsection or reasonably arising from such order; and

(ii) any—

(I) actions taken by customers of such entity to circumvent any restriction on access to the foreign infringing site, or portion thereof, that is subject to such order, that is instituted pursuant to this subsection, or

(II) act, failure, or inability to restrict access to a foreign infringing site, or portion thereof, that is subject to such order, in spite of good faith efforts to comply with such order by such entity,

shall not be used by any person in any claim or cause of action against such entity.

(d) MODIFICATION OR VACATION OF ORDERS.—

(1) IN GENERAL.—At any time after the issuance of an order under subsection (b), a motion to modify, suspend, or vacate the order may be filed by—

(A) any person, or owner or operator of property, that is subject to the order;

(B) any registrant of the domain name, or the owner or operator, of the Internet site that is subject to the order;

(C) any domain name registrar, registry, or other domain name registration authority that has registered or assigned the domain name of the Internet site that is subject to the order; or

(D) any entity that has been served with a copy of an order pursuant to subsection (c) that requires such entity to take action prescribed in that subsection.

(2) RELIEF.—Relief under this subsection shall be proper if the court finds that—

(A) the foreign Internet site subject to the order is no longer, or never was, a foreign infringing site; or

(B) the interests of justice otherwise require that the order be modified, suspended, or vacated.

(3) CONSIDERATION.—In making a relief determination under paragraph (2), a court may consider whether the domain name of the foreign Internet site has expired or has been re-registered by an entity other than the entity that is subject to the order with respect to which the motion under paragraph (1) is brought.

(4) INTERVENTION.—An entity required to take action pursuant to subsection (c) if an order issues under subsection (b) may intervene at any time in any action commenced under subsection (b) that may result in such order, or in any action to modify, suspend, or vacate such order under this subsection.

(e) AMENDED ORDERS.—The Attorney General, if alleging that a foreign Internet site previously adjudicated in an action under this section to be a foreign infringing site is accessible or has been reconstituted at a different domain name or Internet Protocol address, may petition the court to amend the order issued under this section accordingly.

(f) LAW ENFORCEMENT COORDINATION.—

(1) IN GENERAL.—The Attorney General shall inform the Intellectual Property Enforcement Coordinator and the heads of appropriate law enforcement agencies of all court orders issued under subsection (b), and all amended orders issued under subsection (e), regarding foreign infringing sites.

(2) ALTERATIONS.—The Attorney General shall, and the defendant may, inform the Intellectual Property Enforcement Coordinator of the modification, suspension, expiration, or vacation of a court order issued under subsection (b) or an amended order issued under subsection (e).

SEC. 103. MARKET-BASED SYSTEM TO PROTECT U.S. CUSTOMERS AND PREVENT U.S. FUNDING OF SITES DEDICATED TO THEFT OF U.S. PROPERTY.

(a) DEFINITIONS.—In this section:

(1) DEDICATED TO THEFT OF U.S. PROPERTY.—An "Internet site is dedicated to theft of U.S. property" if—

(A) it is an Internet site, or a portion thereof, that is a U.S.-directed site and is used by users within the United States; and

(B) either—

(i) the U.S.-directed site is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in, offering goods or services in a manner that engages in, enables, or facilitates—

(I) a violation of section 501 of title 17, United States Code;

(II) a violation of section 1201 of title 17, United States Code; or

(III) the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark, as that term is defined in section 34(d) of the Lanham Act or section 2320 of title 18, United States Code; or

(ii) the operator of the U.S.-directed site—

(I) is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute a violation of section 501 or 1201 of title 17, United States Code; or

(II) operates the U.S.-directed site with the object of promoting, or has promoted, its use to carry out acts that constitute a violation of section 501 or 1201 of title 17, United States Code,

as shown by clear expression or other affirmative steps taken to foster infringement.

(2) QUALIFYING PLAINTIFF.—The term "qualifying plaintiff" means, with respect to a particular Internet site or portion thereof, a holder of an intellectual property right harmed by the activities described in paragraph (1) occurring on that Internet site or portion thereof.

(b) DENYING U.S. FINANCIAL SUPPORT OF SITES DEDICATED TO THEFT OF U.S. PROPERTY.—

(1) PAYMENT NETWORK PROVIDERS.—Except in the case of an effective counter notification pursuant to paragraph (5), a payment network provider shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after delivery of a notification under paragraph (4), that are designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States and the Internet site, or portion thereof, that is specified in the notification under paragraph (4).

(2) INTERNET ADVERTISING SERVICES.—Except in the case of an effective counter notification pursuant to paragraph (5), an Internet advertising service that contracts with the operator of an Internet site, or portion thereof, that is specified in a notification delivered under paragraph (4), to provide advertising to or for such site or portion thereof, or that knowingly serves advertising to or for such site or portion thereof, shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after delivery the notification under paragraph (4), that are designed to—

(A) prevent its service from providing advertisements to or relating to the Internet site, or portion thereof, that is specified in the notification;

(B) cease making available advertisements for such Internet site, or portion thereof, that is specified in the notification, or paid or sponsored search results, links, or other placements that provide access to such Internet site, or portion thereof, that is specified in the notification; and

(C) cease providing or receiving any compensation for advertising or related services to, from, or in connection with such Internet site, or portion thereof, that is specified in the notification.

(3) DESIGNATED AGENT.—

(A) IN GENERAL.—Each payment network provider and each Internet advertising service shall designate an agent to receive notifications described in paragraph (4), by making available through its service, including on its Web site in a location accessible to the public, and by providing to the Copyright Office, substantially the following:

(i) The name, address, phone number, and electronic mail address of the agent.

(ii) Other contact information that the Register of Copyrights considers appropriate.

(B) DIRECTORY OF AGENTS.—The Register of Copyrights shall maintain and make available to the public for inspection, including through the Internet, in electronic format, a current directory of agents designated under subparagraph (A).

(4) NOTIFICATION REGARDING INTERNET SITES DEDICATED TO THEFT OF U.S. PROPERTY.—

(A) REQUIREMENTS.—Subject to subparagraph (B), a notification under this paragraph is effective only if it is a written communication that is provided to the designated agent of a payment network provider or an Internet advertising service and includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the holder of an intellectual property right harmed by the activities described in subsection (a)(1).

(ii) Identification of the Internet site, or portion thereof, dedicated to theft of U.S. property, including either the domain name or Internet Protocol address of such site, or both.

(iii) Identification of the specific facts to support the claim that the Internet site, or portion thereof, is dedicated to theft of U.S. property and to clearly show that immediate and irreparable injury, loss, or damage will result to the holder of the intellectual property right harmed by the activities described in subsection (a)(1) in the absence of timely action by the payment network provider or Internet advertising service.

(iv) Information reasonably sufficient to establish that the payment network provider or Internet advertising service is providing payment processing or Internet advertising services for such site.

(v) Information reasonably sufficient to permit the payment network provider or Internet advertising service to contact the holder of the intellectual property right harmed by the activities described in subsection (a)(1).

(vi) A statement that the holder of the intellectual property right has a good faith belief that the use of the owner's works or goods in which the right exists, in the manner described in the notification, is not authorized by the holder, its agent, or law.

(vii) A statement that the information in the notification is accurate, and, under penalty of perjury, that the signatory is authorized to act on behalf of the holder of the intellectual property right harmed by the activities described in subsection (a)(1).

(viii) Identification of the evidence indicating that the site (or portion thereof) is a U.S.-directed site.

(B) SERVICE IF NO AGENT DESIGNATED.—If a payment network provider or Internet advertising service has not designated an agent under paragraph (3), the notification under subparagraph (A) may be provided to any officer or legal representative of such provider or service.

(C) NOTICE TO INTERNET SITE IDENTIFIED IN NOTIFICATION.—Upon receipt of an effective notification under this paragraph, a payment network provider or Internet advertising service shall take appropriate steps to ensure timely delivery of the notification to the Internet site identified in the notification.

(5) COUNTER NOTIFICATION.—

(A) REQUIREMENTS.—Subject to subparagraph (B), a counter notification is effective under this paragraph only if it is a written communication that is provided to the designated agent of a payment network provider or an Internet advertising service and includes substantially the following:

(i) A physical or electronic signature of the owner or operator of the Internet site, or portion thereof, specified in a notification under paragraph (4) subject to which action is to be taken by the payment network provider or Internet advertising service under paragraph (1) or (2), or of the registrant of the domain name used by such site or portion thereof.

(ii) In the case of an Internet site specified in the notification under paragraph (4) that is a foreign Internet site, a statement that the owner or operator, or registrant, consents to the jurisdiction of the courts of the United States, and will accept service of process from the person who provided notification under paragraph (4), or an agent of such person, for purposes of adjudicating whether the site is an Internet site dedicated to theft of U.S. property under this section.

(iii) A statement under penalty of perjury that the owner or operator, or registrant, has a good faith belief that it does not meet the criteria of an Internet site dedicated to theft of U.S. property as set forth under this section.

(iv) The name, address, email address, and telephone number of the owner, operator, or registrant.

(B) SERVICE IF NO AGENT DESIGNATED.—If a payment network provider or Internet advertising service has not designated an agent under paragraph (3), the counter notification under subparagraph (A) may be provided to any officer or legal representative of such provider or service.

(6) MISREPRESENTATIONS.—Any provider of a notification or counter notification who knowingly materially misrepresents under this section—

(A) that a site is an Internet site dedicated to the theft of U.S. property, or

(B) that such site does not meet the criteria of an Internet site dedicated to the theft of U.S. property,

shall be liable for damages, including costs and attorneys' fees, incurred by the person injured by such misrepresentation as a result of the misrepresentation.

(c) LIMITED INJUNCTIVE RELIEF IN CASES OF COUNTER NOTIFICATION.—

(1) IN PERSONAM.—If an effective counter notification is made under subsection (b)(5), or if a payment network provider fails to comply with subsection (b)(1), or an Internet advertising service fails to comply with subsection (b)(2), pursuant to a notification under subsection (b)(4) in the absence of such a

counter notification, a qualifying plaintiff may commence an in personam action against—

(A) a registrant of a domain name used by the Internet site, or portion thereof, that is subject to the notification under subsection (b)(4); or

(B) an owner or operator of the Internet site or portion thereof.

(2) IN REM.—If through due diligence a qualifying plaintiff who is authorized to bring an in personam action under paragraph (1) with respect to an Internet site dedicated to theft of U.S. property is unable to find a person described in subparagraphs (A) or (B) of paragraph (1), or no such person found has an address within a judicial district of the United States, the qualifying plaintiff may commence an in rem action against that Internet site or the domain name used by such site.

(3) NOTICE.—Upon commencing an action under this subsection, the qualifying plaintiff shall send a notice of the alleged activity described in subsection (a)(1) and intent to proceed under this subsection—

(A) to the registrant of the domain name of the Internet site, or portion thereof, that is the subject to the notification under subsection (b)(4)—

(i) at the postal and electronic mail addresses appearing in the applicable publicly accessible database of registrations, if any, and to the extent such addresses are reasonably available; and

(ii) via the postal and electronic mail addresses of the registrar, registry, or other domain name registration authority that registered or assigned the domain name of the Internet site, or portion thereof, to the extent such addresses are reasonably available;

(B) to the owner or operator of the Internet site, or portion thereof—

(i) at the primary postal and electronic mail addresses for such owner or operator that are provided on the Internet site, or portion thereof, if any, and to the extent such addresses are reasonably available; or

(ii) if there is no domain name of the Internet site or portion thereof, via the postal and electronic mail addresses of the Internet Protocol allocation entity appearing in the applicable publicly accessible database of allocations and assignments, if any, and to the extent such addresses are reasonably available; or

(C) in any other such form as the court may prescribe, including as may be required by rule 4(f) of the Federal Rules of Civil Procedure.

(4) SERVICE OF PROCESS.—For purposes of this section, the actions described in this subsection shall constitute service of process.

(5) RELIEF.—On application of a qualifying plaintiff following the commencement of an action under this section with respect to an Internet site dedicated to theft of U.S. property, the court may issue a temporary restraining order, a preliminary injunction, or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure, against a registrant of a domain name used by the Internet site, or against an owner or operator of the Internet site, or, in an action brought in rem under paragraph (2), against the Internet site, or against the domain name used by the Internet site, to cease and desist from undertaking any further activity as an Internet site dedicated to theft of U.S. property.

(d) ACTIONS BASED ON COURT ORDERS.—

(1) SERVICE AND RESPONSE.—

(A) SERVICE BY QUALIFYING PLAINTIFF.—A qualifying plaintiff, with the prior approval of the court, may serve a copy of a court order issued under subsection (c) on similarly situated entities described in paragraph (2). Proof of service shall be filed with the court.

(B) RESPONSE.—An entity served under subparagraph (A) shall, not later than 7 days after the date of such service, file with the court a certification acknowledging receipt of a copy of the order and stating that such entity has complied or will comply with the obligations imposed under paragraph (2), or explaining why the entity will not so comply.

(C) VENUE FOR SERVICE.—A copy of the court order may be served in any judicial district where an entity resides or may be found.

(2) REASONABLE MEASURES.—After being served with a copy of an order pursuant to this subsection, the following shall apply:

(A) PAYMENT NETWORK PROVIDERS.—

(i) PREVENTING AFFILIATION.—A payment network provider shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the court order, or within such time as the court may order, that are

designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States or subject to the jurisdiction of the United States and any account—

(I) which is used by the Internet site dedicated to theft of U.S. property that is subject to the order; and

(II) through which the payment network provider would complete such payment transactions.

(ii) NO DUTY TO MONITOR.—A payment network provider is in compliance with clause (i) if it takes action described in that clause with respect to accounts it has as of the date of service of the order, or as of the date of any subsequent notice that its service is being used to complete payment transactions described in clause (i).

(B) INTERNET ADVERTISING SERVICES.—

(i) REQUIRED ACTIONS.—An Internet advertising service that contracts with the Internet site dedicated to theft of U.S. property that is subject to the order to provide advertising to or for such Internet site, or that knowingly serves advertising to or for such internet site, shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, that are designed to—

(I) prevent its service from providing advertisements to or relating to the Internet site;

(II) cease making available advertisements for the Internet site, or paid or sponsored search results, links, or other placements that provide access to the Internet site; and

(III) cease providing or receiving any compensation for advertising or related services to, from, or in connection with the Internet site.

(ii) NO DUTY TO MONITOR.—An internet advertising service is in compliance with clause (i) if it takes action described in that clause with respect to accounts it has as of the date on which a copy of the order is served, or as of the date of any subsequent notice that its service is being used for activities described in clause (i).

(3) COMMUNICATION WITH USERS.—An entity taking an action described in this subsection shall determine the means to communicate such action to the entity's users or customers.

(4) ENFORCEMENT OF ORDERS.—

(A) RULE OF CONSTRUCTION.—The authority under this subsection shall be the sole legal remedy to enforce the obligations of any entity under this subsection.

(B) PROCEDURES AND RELIEF.—

(i) SHOW CAUSE ORDER.—On a showing by the qualifying plaintiff of probable cause to believe that an entity served with a copy of a court order issued under subsection (c) has not complied with its obligations under this subsection by reason of such court order, the court shall require the entity to show cause why an order should not issue—

(I) to require compliance with the obligations of this subsection; and

(II) to impose an appropriate monetary sanction, consistent with the court's exercise of its equitable authority, to enforce compliance with its lawful orders, if the entity—

(aa) has knowingly and willfully failed to file a certification required by paragraph (1)(B);

(bb) has filed such a certification agreeing to comply but has knowingly and willfully failed to do so; or

(cc) has knowingly and willfully certified falsely that compliance with the requirements of paragraph (2) is not required by law.

(ii) SERVICE OF PROCESS.—The order to show cause, and any other process, may be served in any judicial district where the entity resides or may be found.

(C) DEFENSE.—An entity against whom relief is sought under subparagraph (B) may establish an affirmative defense by showing that the entity does not have the technical means to comply with this subsection without incurring an unreasonable economic burden, or that the order is not authorized by this subsection. Such showing shall not be presumed to be a complete defense but shall serve as a defense only for those measures for which

a technical limitation on compliance is demonstrated or for such portions of the order as are demonstrated to be unauthorized by this subsection.

(5) IMMUNITY.—

(A) IMMUNITY FROM SUIT.—Other than in an action pursuant to paragraph (4), no cause of action shall lie in any Federal or State court or administrative agency against any entity served with a copy of a court order issued under subsection (c), or against any director, officer, employee, or agent thereof, for any act reasonably designed to comply with this subsection or reasonably arising from such order.

(B) IMMUNITY FROM LIABILITY.—Other than in an action pursuant to paragraph (4)—

(i) any entity served with a copy of an order under this subsection, and any director, officer, employee, or agent thereof, shall not be liable for any acts reasonably designed to comply with this subsection or reasonably arising from such order; and

(ii) any—

(I) actions taken by customers of such entity to circumvent any restriction on access to the Internet site, or portion thereof that is subject to such order, that is instituted pursuant to this subsection, or

(II) act, failure, or inability to restrict access to an Internet site or portion thereof that is subject to such order, despite good faith efforts to comply with such order by such entity,

shall not be used by any person in any claim or cause of action against such entity.

(e) MODIFICATION OR VACATION OF ORDERS.—

(1) IN GENERAL.—At any time after the issuance of an order under subsection (c), or an amended order issued under subsection (f), with respect to an Internet site dedicated to theft of U.S. property, a motion to modify, suspend, or vacate the order may be filed by—

(A) any person, or owner or operator of property, that is subject to the order;

(B) any registrant of the domain name, or the owner or operator, of such Internet site;

(C) any domain name registrar, registry, or other domain name registration authority that has registered or assigned the domain name of such Internet site; or

(D) any entity that has been served with a copy of an order under subsection (d), or an amended order under subsection (f), that requires such entity to take action prescribed in that subsection.

(2) RELIEF.—Relief under this subsection shall be proper if the court finds that—

(A) the Internet site subject to the order is no longer, or never was, an Internet site dedicated to theft of U.S. property; or

(B) the interests of justice otherwise require that the order be modified, suspended, or vacated.

(3) CONSIDERATION.—In making a relief determination under paragraph (2), a court may consider whether the domain name of the Internet site has expired or has been re-registered by an entity other than the entity that is subject to the order with respect to which the motion under paragraph (1) is brought.

(4) INTERVENTION.—An entity required to take action pursuant to subsection (d) if an order issues under subsection (c) may intervene at any time in any action commenced under subsection (c) that may result in such order, or in any action to modify, suspend, or vacate such order under this subsection.

(f) AMENDED ORDERS.—The qualifying plaintiff, if alleging that an Internet site previously adjudicated in an action under this section to be an Internet site dedicated to theft of U.S. property is accessible or has been reconstituted at a different domain name or Internet Protocol address, may petition the court to amend the order issued under this section accordingly.

(g) REPORTING OF ORDERS.—

(1) IN GENERAL.—The qualifying plaintiff shall inform the Intellectual Property Enforcement Coordinator of any court order issued under subsection (c) or amended order issued under subsection (f).

(2) ALTERATIONS.—Upon the modification, suspension, expiration, or vacation of a court order issued under subsection (c) or an amended order issued under subsection (f), the qualifying plaintiff shall, and the defendant may, so inform the Intellectual Property Enforcement Coordinator.

SEC. 104. IMMUNITY FOR TAKING VOLUNTARY ACTION AGAINST SITES DEDICATED TO THEFT OF U.S. PROPERTY.

No cause of action shall lie in any Federal or State court or administrative agency against, no person may rely in any claim or cause of action against, and no liability for damages to any person shall be granted against, a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for taking any action described in section 102(c)(2), section 103(d)(2), or section 103(b) with respect to an Internet site, or otherwise voluntarily blocking access to or ending financial affiliation with an Internet site, in the reasonable belief that—

(1) the Internet site is a foreign infringing site or is an Internet site dedicated to theft of U.S. property; and

(2) the action is consistent with the entity's terms of service or other contractual rights.

SEC. 105. IMMUNITY FOR TAKING VOLUNTARY ACTION AGAINST SITES THAT ENDANGER PUBLIC HEALTH.

(a) REFUSAL OF SERVICE.—A service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar, acting in good faith and based on credible evidence, may stop providing or refuse to provide services to an Internet site that endangers the public health.

(b) IMMUNITY FROM LIABILITY.—An entity described in subsection (a), including its directors, officers, employees, or agents, that ceases or refuses to provide services under subsection (a) shall not be liable to any person under any Federal or State law for such action.

(c) DEFINITIONS.—In this section:

(1) ADULTERATED.—The term "adulterated" has the meaning given that term in section 501 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351).

(2) INTERNET SITE THAT ENDANGERS THE PUBLIC HEALTH.—The term "Internet site that endangers the public health" means an Internet site that is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in—

(A) offering, selling, dispensing, or distributing any prescription medication, and does so regularly without a valid prescription; or

(B) offering, selling, dispensing, or distributing any prescription medication that is adulterated or misbranded.

(3) MISBRANDED.—the term "misbranded" has the meaning given that term in section 502 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 352).

(4) PRESCRIPTION MEDICATION.—

(A) PRESCRIPTION MEDICATION.—The term "prescription medication" means a drug that is subject to section 503(b) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 353(b)).

(B) DRUG.—The term "drug" has the meaning given that term in section 201(g)(1) of the Federal Food Drug, and Cosmetic Act (21 U.S.C. 321(g)(1)).

(5) VALID PRESCRIPTION.—The term "valid prescription" has the meaning given that term in section 309(e)(2)(A) of the Controlled Substances Act (21 U.S.C. 829(e)(2)(A)).

SEC. 106. GUIDELINES AND STUDY.

(a) GUIDELINES.—The Attorney General shall—

(1) provide appropriate resources and procedures for case management and development to effect timely disposition of actions brought under this title;

(2) develop a deconfliction process in consultation with appropriate law enforcement agencies, including U.S. Immigration and Customs Enforcement, to coordinate enforcement activities under this title;

(3) publish procedures developed in consultation with appropriate law enforcement agencies, including U.S. Immigration and Customs Enforcement, to receive information from the public relevant to the enforcement of this title; and

(4) provide guidance to intellectual property rights holders about what information such rights holders should provide to assist in initiating an investigation or to supplement an ongoing investigation pursuant to this title.

(b) STUDY.—

(1) NATURE OF STUDY.—The Register of Copyrights, in consultation with appropriate departments and agencies of the United States and other stakeholders, shall conduct a study on the enforcement and effectiveness of this title

and on any need to amend the provisions of this title to adapt to emerging technologies.

(2) REPORTS TO CONGRESS.—Not later than 2 years after the date of the enactment of this Act, the Register of Copyrights shall submit to the Committees on the Judiciary of the House of Representatives and the Senate a report containing the results of the study conducted under this subsection and any recommendations that the Register may have as a result of the study.

SEC. 107. DENYING U.S. CAPITAL TO NOTORIOUS FOREIGN INFRINGERS.

(a) IDENTIFICATION AND RECOMMENDATIONS REGARDING NOTORIOUS FOREIGN INFRINGERS.—

(1) IN GENERAL.—Using existing resources, the Intellectual Property Enforcement Coordinator, in consultation with the Secretaries of Treasury and Commerce, the United States Trade Representative, the Chairman of the Securities and Exchange Commission, and the heads of other departments and appropriate agencies, shall identify and conduct an analysis of notorious foreign infringers whose activities cause significant harm to holders of intellectual property rights in the United States.

(2) PUBLIC INPUT.—In carrying out paragraph (1), the Intellectual Property Enforcement Coordinator shall solicit and give consideration to the views and recommendations of members of the public, including holders of intellectual property rights in the United States.

(b) REPORT TO CONGRESS.—The Intellectual Property Enforcement Coordinator shall, not later than 6 months after the date of the enactment of this Act, submit to the Committees on the Judiciary of the House of Representatives and the Senate a report that includes the following:

(1) An analysis of notorious foreign infringers and a discussion of how these infringers violate industry norms regarding the protection of intellectual property.

(2) An analysis of the significant harm inflicted by notorious foreign infringers on consumers, businesses, and intellectual property industries in the United States and abroad.

(3) An examination of whether notorious foreign infringers have attempted to or succeeded in accessing capital markets in the United States for funding or public offerings.

(4) An analysis of the adequacy of relying upon foreign governments to pursue legal action against notorious foreign infringers.

(5) A discussion of specific policy recommendations to deter the activities of notorious foreign infringers and encourage foreign businesses to adopt industry norms that promote the protection of intellectual property globally, including addressing—

(A) whether notorious foreign infringers that engage in significant infringing activity should be prohibited by the laws of the United States from seeking to raise capital in the United States, including offering stock for sale to the public; and

(B) whether the United States Government should initiate a process to identify and designate foreign entities from a list of notorious foreign infringers that would be prohibited from raising capital in the United States.

TITLE II—ADDITIONAL ENHANCEMENTS TO COMBAT INTELLECTUAL PROPERTY THEFT

SEC. 201. STREAMING OF COPYRIGHTED WORKS IN VIOLATION OF CRIMINAL LAW.

(a) TITLE 17 AMENDMENTS.—Section 506(a) of title 17, United States Code, is amended to read as follows:

"(a) CRIMINAL INFRINGEMENT.—

"(1) IN GENERAL.—Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed—

"(A) for purposes of commercial advantage or private financial gain;

"(B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, or by the public performance by means of digital transmission, during any 180-day period, of 1 or more copyrighted works, when the total retail value of the copies or phonorecords, or of the public performances, is more than $1,000; or

"(C) by the distribution or public performance of a work being prepared for commercial dissemination, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial dissemination.

"(2) EVIDENCE.—For purposes of this subsection, evidence of reproduction, distribution, or public performance of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

"(3) DEFINITION.—In this subsection, the term 'work being prepared for commercial dissemination' means—

"(A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution or public performance—

"(i)(I) the copyright owner has a reasonable expectation of commercial distribution; and

"(II) the copies or phonorecords of the work have not been commercially distributed in the United States by or with the authorization of the copyright owner; or

"(ii)(I) the copyright owner does not intend to offer copies of the work for commercial distribution but has a reasonable expectation of other forms of commercial dissemination of the work; and

"(II) the work has not been commercially disseminated to the public in the United States by or with the authorization of the copyright owner;

"(B) a motion picture, if, at the time of unauthorized distribution or public performance, the motion picture—

"(i)(I) has been made available for viewing in a motion picture exhibition facility; and

"(II) has not been made available in copies for sale to the general public in the United States by or with the authorization of the copyright owner in a format intended to permit viewing outside a motion picture exhibition facility; or

"(ii) had not been commercially disseminated to the public in the United States by or with the authorization of the copyright owner more than 24 hours before the unauthorized distribution or public performance.".

(b) TITLE 18 AMENDMENTS.—Section 2319 of title 18, United States Code, is amended—

(1) in subsection (b)(1), by striking "during any 180-day period" and all that follows and insert "of at least 10 copies or phonorecords, or of at least 10 public performances by means of digital transmission, of 1 or more copyrighted works, during any 180-day period, which have a total retail value of more than $2,500;";

(2) in subsection (c)—

(A) in paragraph (1), by striking "of 10 or more copies or phonorecords" and all that follows and inserting "including by electronic means, of at least 10 copies or phonorecords, or of at least 10 public performances by means of digital transmission, of 1 or more copyrighted works, during any 180-day period, which have a total retail value of more than $2,500;"; and

(B) in paragraph (3), by striking "if the offense" and all that follows and inserting "in any other case;";

(3) in subsection (d)(4), by striking "under paragraph (2)" and inserting "committed for purposes of commercial advantage or private financial gain under subsection (a)";

(4) in subsection (f)—

(A) by amending paragraph (2) to read as follows:

"(2) the terms 'reproduction', 'distribution', and 'public performance' refer to the exclusive rights of a copyright owner under paragraphs (1), (3), (4), and (6), respectively, of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17; and";

(B) in paragraph (3), by striking "; and" and inserting a period; and

(C) by striking paragraph (4); and

(5) by adding at the end the following new subsection:

"(g) EVIDENCE OF TOTAL RETAIL VALUE.—For purposes of this section and section 506(a) of title 17, total retail value may be shown by evidence of—

"(1) the total retail price that persons receiving the reproductions, distributions, or public performances constituting the offense would have paid to receive such reproductions, distributions, or public performances lawfully;

"(2) the total economic value of the reproductions, distributions, or public performances to the infringer or to the copyright owner, as shown by evidence of fee, advertising, or other revenue that was received by the person who commits the offense, or that the copyright owner would have been entitled to receive had such reproductions, distributions, or public performances been offered lawfully; or

"(3) the total fair market value of licenses to offer the type of reproductions, distributions, or public performances constituting the offense.".

(c) RULE OF CONSTRUCTION.—Any person acting with a good faith reasonable basis in law to believe that the person's conduct is lawful shall not be considered to have acted willfully for purposes of the amendments made by this section. Such person includes, but is not limited to, a person engaged in conduct forming the basis of a bona fide commercial dispute over the scope of existence of a contract or license governing such conduct where such person has a reasonable basis in law to believe that such conduct is noninfringing. Nothing in this subsection shall affect the application or interpretation of the willfulness requirement in any other provision of civil or criminal law.

SEC. 202. TRAFFICKING IN INHERENTLY DANGEROUS GOODS OR SERVICES.

Section 2320 of title 18, United States Code, is amended as follows:

(1) Subsection (a) is amended to read as follows:

"(1) IN GENERAL.—

"(A) OFFENSES.—Whoever—

"(i) intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services,

"(ii) intentionally traffics or attempts to traffic in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive, or

"(iii) intentionally imports, exports, or traffics in counterfeit drugs or intentionally participates in or knowingly aids drug counterfeiting,

shall, if an individual, be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined not more than $5,000,000.

"(B) SUBSEQUENT OFFENSES.—In the case of an offense by a person under this paragraph that occurs after that person is convicted of another offense under this paragraph, the person convicted, if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000.

"(2) SERIOUS BODILY HARM OR DEATH.—

"(A) SERIOUS BODILY HARM.—If the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of paragraph (1), the penalty shall be, for an individual, a fine of not more than $5,000,000 or imprisonment for any term of years or for life, or both, and for other than an individual, a fine of not more than $15,000,000.

"(B) DEATH.—If the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of paragraph (1), the penalty shall be, for an individual, a fine of not more than $5,000,000 or imprisonment for any term of years or for life, or both, and for other than an individual, a fine of not more than $15,000,000.

"(3) MILITARY GOODS OR SERVICES.—

"(A) IN GENERAL.—A person who commits an offense under paragraph (1) shall be punished in accordance with subparagraph (B) if—

"(i) the offense involved a good or service described in paragraph (1) that if it malfunctioned, failed, or was compromised, could reasonably be foreseen to cause—

"(I) serious bodily injury or death;

"(II) disclosure of classified information;

"(III) impairment of combat operations; or

"(IV) other significant harm—

"(aa) to a member—

"(AA) of the Armed Forces; or

"(BB) of a Federal, State, or local law enforcement agency; or

"(bb) to national security or critical infrastructure; and

"(ii) the person had knowledge that the good or service is falsely identified as meeting military standards or is intended for use in a military or national security application, or a law enforcement or critical infrastructure application.

"(B) PENALTIES.—

"(i) INDIVIDUAL.—An individual who commits an offense described in subparagraph (A) shall be fined not more than $5,000,000, imprisoned for not more than 20 years, or both.

"(ii) PERSON OTHER THAN AN INDIVIDUAL.—A person other than an individual that commits an offense described in subparagraph (A) shall be fined not more than $15,000,000.

"(C) SUBSEQUENT OFFENSES.—

"(i) INDIVIDUAL.—An individual who commits an offense described in subparagraph (A) after the individual is convicted of an offense under subparagraph (A) shall be fined not more than $15,000,000, imprisoned not more than 30 years, or both.

"(ii) PERSON OTHER THAN AN INDIVIDUAL.—A person other than an individual that commits an offense described in subparagraph (A) after the person is convicted of an offense under subparagraph (A) shall be fined not more than $30,000,000.".

(2) Subsection (e) is amended—

(A) in paragraph (1), by striking the period at the end and inserting a semicolon;

(B) in paragraph (3), by striking "and" at the end;

(C) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(D) by adding at the end the following:

"(5) the term 'counterfeit drug' has the meaning given that term in section 201(g)(2) of the Federal Food Drug, and Cosmetic Act (21 U.S.C. 321(g)(2));

"(6) the term 'critical infrastructure' has the meaning given that term in section 2339D(c);

"(7) the term 'drug counterfeiting' means any act prohibited by section 301(i) of the Federal Food Drug, and Cosmetic Act (21 U.S.C. 331(i));

"(8) the term 'final dosage form' has the meaning given that term in section 735(4) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 379g(4));

"(9) the term 'falsely identified as meeting military standards' relating to a good or service means there is a material misrepresentation that the good or service meets a standard, requirement, or specification issued by the Department of Defense, an Armed Force, or a reserve component;

"(10) the term 'use in a military or national security application' means the use of a good or service, independently, in conjunction with, or as a component of another good or service—

"(A) during the performance of the official duties of the Armed Forces of the United States or the reserve components of the Armed Forces; or

"(B) by the United States to perform or directly support—

"(i) combat operations; or

"(ii) critical national defense or national security functions; and

"(11) the term 'use in a law enforcement or critical infrastructure application' means the use of a good or service, independently, in conjunction with, or as a component of, another good or service by a person who is directly engaged in—

"(A) Federal, State, or local law enforcement; or

"(B) an official function pertaining to critical infrastructure.".

SEC. 203. PROTECTING U.S. BUSINESSES FROM FOREIGN AND ECONOMIC ESPIONAGE.

(a) FOR OFFENSES COMMITTED BY INDIVIDUALS.—Section 1831(a) of title 18, United States Code, is amended, in the matter after paragraph (5)—

(1) by striking "15 years" and inserting "20 years"; and

(2) by striking "not more than $500,000" and inserting "not less than $1,000,000 and not more than $5,000,000".

(b) FOR OFFENSES COMMITTED BY ORGANIZATIONS.—Section 1831(b) of such title is amended by striking "$10,000,000" and inserting "not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization (including expenses for research and design or other costs of reproducing the trade secret that the organization has thereby avoided)".

SEC. 204. AMENDMENTS TO SENTENCING GUIDELINES.

Not later than 180 days after the date of the enactment of this Act, pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall—

(1) review, and if appropriate, amend Federal Sentencing Guidelines and policy statements applicable to persons convicted of—

(A) intellectual property offenses;

(B) an offense under section 2320(a) of title 18, United States Code; or

(C) an offense under section 1831 of title 18, United States Code;

(2) in carrying out such review, consider amending such Guidelines and policy statements to—

(A) apply an appropriate offense level enhancement for intellectual property offenses committed in connection with an organized criminal enterprise;

(B) apply an appropriate offense level enhancement to the simple misappropriation of a trade secret;

(C) apply an additional appropriate offense level enhancement if the defendant transmits or attempts to transmit the stolen trade secret outside of the United States and an additional appropriate enhancement if the defendant instead commits economic espionage;

(D) provide that when a defendant transmits trade secrets outside of the United States or commits economic espionage, that the defendant should face a minimum offense level;

(E) provide for an offense level enhancement for Guidelines relating to the theft of trade secrets and economic espionage, including trade secrets transferred or attempted to be transferred outside of the United States;

(F) apply an appropriate offense level enhancement and minimum offense level for offenses under section 2320(a) of title 18, United States Code, that involve a product intended for use in a military or national security application, or a law enforcement or critical infrastructure application;

(G) ensure that the Guidelines and policy statements (including section 2B5.3 of the Federal Sentencing Guidelines (and any successor thereto)) reflect—

(i) the serious nature of the offenses described in section 2320(a) of title 18, United States Code;

(ii) the need for an effective deterrent and appropriate punishment to prevent offenses under section 2320(a) of title 18, United States Code; and

(iii) the effectiveness of incarceration in furthering the objectives described in clauses (i) and (ii); and

(H) ensure reasonable consistency with other relevant directives and Guidelines and Federal statutes;

(3) submit to Congress a report detailing the Commission's actions with respect to each potential amendment described in paragraph (2);

(4) make such conforming amendments to the Federal Sentencing Guidelines as the Commission determines necessary to achieve consistency with other Guideline provisions and applicable law; and

(5) promulgate the Guidelines, policy statements, or amendments provided for in this section as soon as practicable in accordance with the procedure set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note), as though the authority under that Act had not expired.

SEC. 205. DEFENDING INTELLECTUAL PROPERTY RIGHTS ABROAD.

(a) RESOURCES TO PROTECT INTELLECTUAL PROPERTY RIGHTS.—

(1) POLICY.—The Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, shall ensure that the protection in foreign countries of the intellectual property rights of United States persons is a significant component of United States foreign and commercial policy in general, and in relations with individual countries in particular.

(2) DEDICATION OF RESOURCES.—The Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, and the heads of other appropriate departments and agencies, shall ensure that adequate resources are available at the United States embassy or diplomatic mission (as the case may be) in any country that is identified under section 182(a)(1) of the Trade Act of 1974 (19 U.S.C. 2242(a)(1)) to ensure—

(A) aggressive support for enforcement action against violations of the intellectual property rights of United States persons in such country;

(B) cooperation with and support for the host government's efforts to conform its applicable laws, regulations, practices, and processes to enable the host government to honor its international and bilateral obligations with respect to the protection of intellectual property rights;

(C) consistency with the policy and country-specific priorities set forth in the most recent report of USTR under such section 182(a)(1); and

(D) support for holders of United States intellectual property rights and industries whose access to foreign markets is improperly restricted by intellectual property related issues.

(b) NEW APPOINTMENTS.—

(1) APPOINTMENTS AND ADMINISTRATION.—The Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, shall appoint at least one intellectual property attaché to be assigned to the United States embassy or diplomatic mission (as the case may be) in a country in each geographic region covered by a regional bureau of the Department of State. The Director of the Patent and Trademark Office shall maintain authority over hiring, personnel ratings, and objectives for the attachés, in consultation with the Secretary of State. Depending on experience and expertise, intellectual property attachés shall be designated as the diplomatic rank in-mission of First Secretary or Counselor.

(2) REGIONS DEFINED.—The geographic regions referred to in paragraph (1) are the following:

(A) Africa.
(B) Europe and Eurasia.
(C) East Asia and the Pacific.
(D) The Near East.
(E) South and Central Asia and the Pacific.
(F) The Western Hemisphere.

(3) DUTIES.—The intellectual property attachés appointed under this subsection shall focus primarily on intellectual property matters, including the development, protection, and enforcement of applicable law. Each intellectual property attaché shall work, in accordance with guidance from the Director, and in coordination with appropriate staff at the Departments of Commerce and State and the Copyright Office, to advance the policy goals and priorities of the United States Government. Those policy goals and priorities shall be consistent with USTR's reports under section 182(a)(1) of the Trade Act of 1974. The intellectual property attachés shall work with United States holders of intellectual property rights and industry to address intellectual property rights violations in the countries where the attachés are assigned.

(c) PRIORITY ASSIGNMENTS.—

(1) IN GENERAL.—Subject to paragraph (2), in designating the United States embassies or diplomatic missions where attachés will be assigned under subsection (b), the Secretary of State and the Secretary of Commerce shall give priority to countries where the activities of an attaché are likely to achieve the greatest potential benefit in reducing intellectual property infringement in the United States market, to advance the intellectual property rights of United States persons and their licensees, and to advance the interests of United States persons who may otherwise be harmed by violations of intellectual property rights in those countries.

(2) ASSIGNMENTS TO PRIORITY COUNTRIES.—In carrying out paragraph (1), the Secretary of State and the Secretary of Commerce shall consider assigning intellectual property attachés—

(A) to the countries that have been identified under section 182(a)(1) of the Trade Act of 1974 (19 U.S.C. 2242(a)(1)); and

(B) to countries of critical economic importance to the advancement of United States intellectual property rights and interests.

(d) TRAINING.—The Secretary of State and the Secretary of Commerce shall ensure that each intellectual property attaché appointed under subsection (b) is fully trained for the responsibilities of the position before assuming duties at the United States embassy or diplomatic mission to which the attaché is assigned.

(e) COORDINATION.—The activities of intellectual property attachés under this section shall be determined in consultation with the Intellectual Property Enforcement Coordinator. The Director shall assist in coordinating the policy priorities and activities of the intellectual property attachés and oversee administrative and personnel matters.

(f) TRAINING AND TECHNICAL ASSISTANCE.—

(1) CONSISTENCY.—Using existing resources, all training and technical assistance provided by intellectual property attachés appointed under subsection

(b), or under other authority, relating to intellectual property enforcement and protection abroad shall be designed to be consistent with the policy and country-specific priorities set forth in the most recent report of USTR under section 182(a) of the Trade Act of 1974.

(2) ROLE OF IPEC.—Such training and technical assistance programs shall be carried out in consultation with the Intellectual Property Enforcement Coordinator. The Director shall assist in coordinating the training and technical assistance programs conducted by intellectual property attachés.

(g) ACTIVITIES IN OTHER COUNTRIES.—In the case of countries that are not identified under section 182(a)(1) of the Trade Act of 1974, the activities of Federal departments and agencies with respect to intellectual property rights in those countries, intellectual property programs and outreach of the United States Government in those countries, and training and technical assistance programs of the United States Government relating to intellectual property in those countries may be conducted to the extent they are consistent with compelling commercial or foreign policy interests of the United States.

(h) REPORTS TO CONGRESS.—The Intellectual Property Enforcement Coordinator shall include in the annual report submitted under section 314 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (15 U.S.C. 8114) on the activities of the advisory committee established under section 301 of that Act (15 U.S.C. 8111) information on the appointment, designation for assignment, and activities of all intellectual property attachés of any Federal department or agency who are serving abroad.

(i) DEFINITIONS.—In this section:

(1) DIRECTOR.—The terms "Director of the Patent and Trademark Office" and "Director" mean the Under Secretary for Intellectual Property and Director of the Untied States Patent and Trademark Office.

(2) INTELLECTUAL PROPERTY ENFORCEMENT.—The term "intellectual property enforcement" has the meaning given that term in section 302 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (15 U.S.C. 8112).

(3) INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR.—The term "Intellectual Property Enforcement Coordinator" means the Intellectual Property Enforcement Coordinator appointed under section 301 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (15 U.S.C. 8111).

(4) INTELLECTUAL PROPERTY RIGHTS.—The term "intellectual property rights" means the rights of holders of copyrights, patents, trademarks, other forms of intellectual property, and trade secrets.

(5) USTR.—The term "USTR" means the United States Trade Representative.

(6) UNITED STATES PERSON.—The term "United States person" means—

(A) any United States resident or national;

(B) any corporation, partnership, other business entity, or other organization, that is organized under the laws of the United States; and

(C) any foreign subsidiary or affiliate (including any permanent foreign establishment) of any corporation, partnership, business entity, or organization described in subparagraph (B), that is controlled in fact by such corporation, partnership, business entity, or organization.

(j) AUTHORIZATION OF APPROPRIATIONS.—The Secretary of State and the Secretary of Commerce shall provide for the training and support of the intellectual property attachés appointed under subsection (b) using existing resources.

○

Mr. CONYERS. Thank you, Chairman Smith, and good morning to my fellow colleagues on the Committee. This is a very important hearing, and I want to commend you on your statement, because you raise some issues that I think we will have to go into quite carefully.

Now, there have been attempts to deal with the problem that is before us today. But HR 3261, the "Stop Online Piracy Act," represents a great deal of work and some experience from our attempts to deal with this subject before.

I am very pleased that this is a bipartisan bill, and I think that is very important.

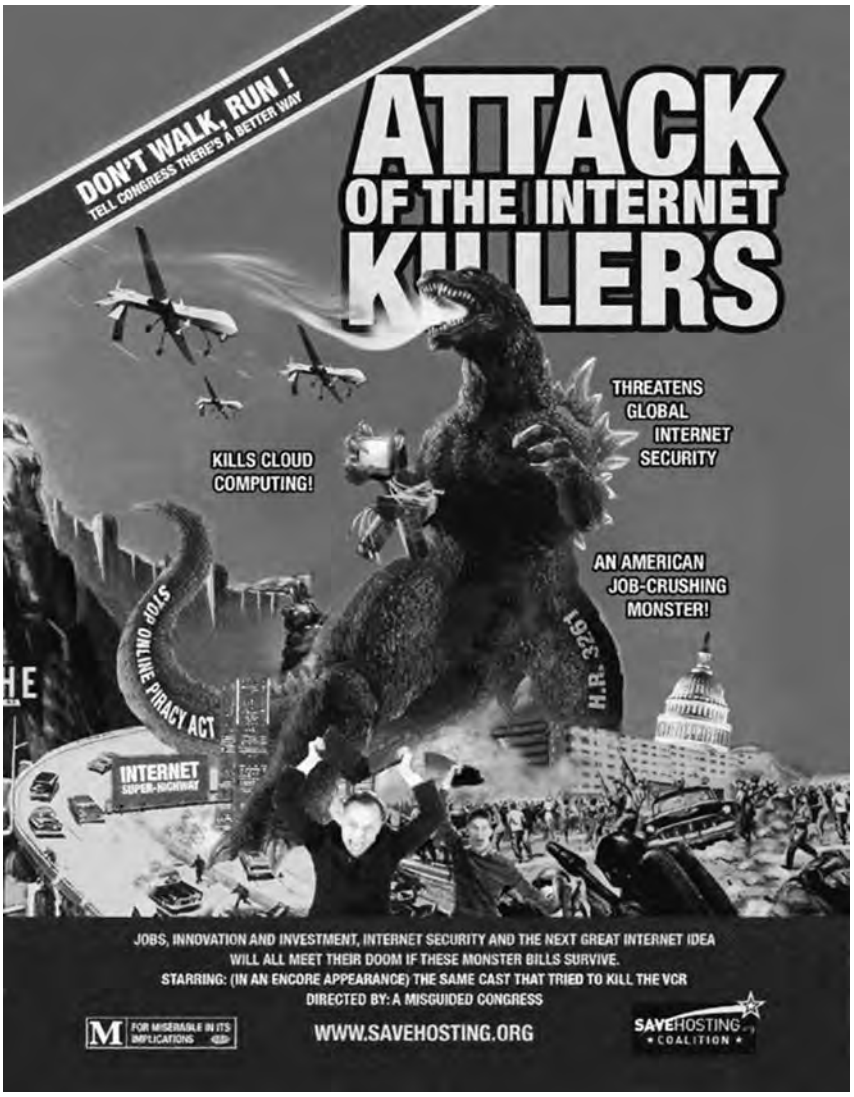
Now, there have been a number of attempts to stop online intellectual property theft and fraud. Some of the leading Internet service providers and right holders, and the best practices standards that are being developed with in the advertising network and payment processing companies, and particularly MasterCard, have all come to my intention. I commend them. But this private cooperation is not sufficient. Our studies have shown that upwards of one-quarter of all Internet traffic is copyright infringing. And to those who say that a bill to stop online theft will break the Internet, I would like to point out that it is not likely to happen.

Users connect to the Internet through service providers, like AT&T and Verizon, but by most accounts, and I have to bring up Google's name again in the beginning of this discussion, Google's search engine connects users to Internet content more often than any other, and places the most advertisements. As users surf the web, their computers, connect with domain name servers to resolve the site name that they type into their browser and its location on the web.

Now, we are getting a number of reactions from this proposal. Some rightsholders have said that the market based process outlined in Section 103 of the bill does not go far, and too many players who profit from piracy. But on the other hand, there are some in the technology sector that have said this bill will break the Internet and strangle startups and Silicon Valley giants alike. And so, I reluctantly asked to put this into the record, "The attack of the Internet killers."

Mr. SMITH. Without objection, that will be made a part of the record.

[The information referred to follows:]



Mr. CONYERS. It is very serious business. "Do not walk, run." "Tell Congress there is a better way." "Threatens global Internet security." "Kills cloud computers." "An American job crushing monster." That is our bill, H.R. 3261.

Mr. SMITH. Is that not a comic?

Mr. CONYERS. No, this is serious. [Laughter.]

It is a terrible thing, and that we ought to know better.

Now, on a more serious note, we have from our friends in the American Civil Liberties Union a caution that I have to take more seriously because they have some questions that I think needs to be examined here, and that is, the first one is that there is an At-

torney General section of the bill that only the Justice Department, in its wisdom, can ask a court to filter or block web content. What the American Civil Liberties Union is telling us is that we will, with this legislation, inadvertently involve non-infringing operators, and that this would violate their constitutional rights.

Now, against that, I am going to ask to put in the imminent First Amendment scholar, Floyd Abrams', recommendation that says that the notion that this bill threatens freedom of expression is unsupportable. It protects creators of free speech, as Congress has done and the Judiciary Committee especially has been particularly sensitive to protecting. And so, I ask unanimous consent to put in the statement of attorney Floyd Abrams. And I yield back the balance of my time. Thank you.

Mr. SMITH. Without objection.

[The information referred to follows:]

CAHILL GORDON & REINDEL LLP
EIGHTY PINE STREET
NEW YORK, NY 10005-1702

FLOYD ABRAMS
L. HOWARD ADAMS
ROBERT A. ALESSI
HELENE R. BANKS
LANDIS C. BEST
SUSAN BUCKLEY
KEVIN J. BURKE
JAMES J. CLARK
BENJAMIN J. COHEN
CHRISTOPHER T. COX
STUART G. DOWNING
ADAM M. DWORKIN
JENNIFER B. EZRING
PATRICIA FARREN
JOAN MURTAGH FRANKEL
JONATHAN J. FRANKEL
BART FRIEDMAN
CIRO A. GAMBONI

WILLIAM B. GANNETT
CHARLES A. GILMAN
STEPHEN A. GREENE
ROBERT M. HALLMAN
WILLIAM M. HARTNETT
CRAIG M. HOROWITZ
DOUGLAS S. HOROWITZ
DAVID G. JANUSZEWSKI
ELAI KATZ
THOMAS J. KAVALER
BRIAN S. KELLEHER
DAVID N. KELLEY
CHÉRIE R. KISER*
EDWARD P. KRUGMAN
JOEL KURTZBERG
ALIZA R. LEVINE
JOEL H. LEVITIN
GEOFFREY E. LIEBMANN

TELEPHONE: (212) 701-3000
FACSIMILE: (212) 269-5420

1990 K STREET, N.W.
WASHINGTON, DC 20006-1181
(202) 862-8900
FAX: (202) 862-8958

AUGUSTINE HOUSE
6A AUSTIN FRIARS
LONDON, ENGLAND EC2N 2HA
(011) 44.20.7920.9800
FAX: (011) 44.20.7920.9825

WRITER'S DIRECT NUMBER
(212) 701-3621

MICHAEL MACRIS
ANN S. MAKICH
JONATHAN I. MARK
BRIAN T. MARKLEY
GERARD M. MEISTRELL
WILLIAM J. MILLER
ATHY A. MOBILIA
NOAH B. NEWITZ
MICHAEL J. OHLER
DAVID R. OWEN
JOHN PAPACHRISTOS
LUIS R. PENALVER
DEAN RINGEL
JAMES ROBINSON
THORN ROSENTHAL
TAMMY L. ROY
JONATHAN A. SCHAFFZIN
JOHN SCHUSTER

MICHAEL A. SHERMAN
DARREN SILVER
HOWARD G. SLOANE
SUSANNA M. SUH
ANTHONY K. TAMA
JONATHAN D. THIER
JOHN A. TRIPODORO
GLENN J. WALDRIP, JR.
MICHAEL B. WEISS
S. PENNY WINDLE
COREY WRIGHT
DANIEL J. ZUBKOFF
ADAM ZUROFSKY

*ADMITTED IN DC ONLY

November 7, 2011

Chairman Lamar Smith
Ranking Member John Conyers
Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, D.C. 20515

Re: Stop Online Piracy Act

Dear Chairman Smith and Ranking Member Conyers:

I write with regard to the Stop Online Piracy Act (H.R. 3261), which is currently under consideration by this Committee.[1] I represent the Directors Guild of America, the American Federation of Television and Radio Artists, the Screen Actors Guild, the International Alliance of Theatrical and Stage Employees, and the Motion Picture Association. I write to you at their request to offer my view that this legislation is consistent with the First Amendment and to set forth the basis for that conclusion.

[1] I have previously written letters to the Senate Judiciary Committee regarding the Protect IP Act, on May 24, 2011, and the Combating Online Infringement and Counterfeits Act (COICA), which was reported out of the Judiciary Committee during the 111th Congress (S. 3804 (Reported in Senate)).

In this letter, I will summarize the provisions of the statute briefly and then turn to its constitutionality under the First Amendment. I think it useful, however, to begin with some observations about copyright law and the First Amendment in the age of the Internet.

I start with what should not be controversial. The Internet is one of the greatest tools of freedom in the history of the world. That is why, as Secretary of State Clinton has observed, there is an "urgent need" to protect freedom of expression on the Internet throughout the world. At the same time, however, she pointed out that "all societies recognize that freedom of expression has its limits," observing specifically that those who use the Internet to "distribute stolen intellectual property cannot divorce their online actions from their real world identities" and that our ability to "safeguard billions of dollars in intellectual property [is] at stake if we cannot rely on the security of our information networks."

It is no answer to this challenge to treat loose metaphors—the Internet as "the Wild West," for example—as substitutes for serious legal analysis. It is one thing to say that the Internet must be free; it is something else to say that it must be lawless. Even the Wild West had sheriffs, and even those who use the Internet must obey duly adopted laws.

It is thus no surprise that libel law applies to material that appears on the Internet. *Milum* v. *Banks*, 642 S.E.2d 892 (Ga. Ct. App. 2007) (holding that defendant published libelous statements by posting them on his website) *cert. denied* (June 4, 2007). Or that libel precedents regarding printing information on paper are given comparable meaning as to information posted online. *Nationwide Bi-Weekly Administration, Inc.* v. *Belo Corp.*, 512 F.3d 137 (5th Cir. 2007) (holding that the "single publication rule" for the statute of limitations in libel suits applies to Internet publication). Or that principles of privacy law are applied to personal information posted online with the same animating principles that apply in more traditional media. *Yath* v. *Fairview Clinics, N.P.*, 767 N.W.2d 34 (Minn. Ct. Ap. 2009) (holding that posting information from a patient's medical file on a social networking website constitutes the "publicity" element of invasion of privacy); *Benz* v. *Washington Newspaper Publishing Co.*, 2006 WL 2844896 (D.D.C. Sept. 29, 2006) (holding that false information posted on independent websites provided reasonable claim for defamation, invasion of privacy and false light against private party defendant, in addition to claims regarding publication of related information by a newspaper).

Copyright law is no different. It is not disputable that "[a]ll existing copyright protections are applicable to the Internet." Edward H. Rosenthal, *J.D. Salinger and Other Reflections on Fair Use*, 1003 PLI/Pat 35, 42 (2010). *See Video Pipeline, Inc.* v. *Buena Vista Home Entertainment, Inc.*, 342 F.3d 191 (3d Cir. 2003) (upholding preliminary injunction against website compiling video clips of copyrighted movies for commercial use); *UMG Recordings, Inc.* v. *Stewart*, 461 F. Supp. 2d 837 (S.D. Ill. 2006) (finding *prima facie* case of liability in support of default judgment against Internet user who downloaded, reproduced and distributed copyrighted audio recordings online). The seizure provisions of copyright laws are applied to seize and stop the use of online property to facilitate infringement, such as domain names, just as offline property can be seized to stop its use to facilitate infringement. *United States* v. *The Following Domain Names: TVShack.net et al.*, 2010 WL

2666284 (S.D.N.Y. June 29, 2010) (treating domain names hosting infringing videos as forfeitable property under 18 U.S.C. §§ 2323(a) and ordering their seizure, locking domain names at registry level, replacing registrar information to identify the government as the domain names' owner, and compelling the registry to route traffic to the domain names to a government IP address notifying the public that the domain name was seized). While Congress has created safe harbors to accommodate the invention of online service providers, it has clearly declined to "simply rewrite copyright law for the on-line world." Copyright claims online are thus "generally evaluated just as they would be in the non-online world." *Ellison* v. *Robertson*, 357 F.3d 1072 (9th Cir. 2004) (internal quotations omitted).

Copyright law has existed throughout our Nation's history. The Constitution itself authorizes Congress to adopt copyright legislation (Art. I, Sec. 8, Clause 8) and the first such legislation was enacted in 1790, a year before the First Amendment was approved by Congress. Ch. 15, 1 Stat. 124 (1790) (repealed). From the start, injunctions were one form of relief accorded to victims of copyright infringement. (Courts applied the 1790 Act, and its later amendments, to grant injunctions "according to principles of equity." Act of Feb. 3, 1831, ch. 16, 4 Stat. at 438 (1831) (repealed 1870) (cited in Kristina Rosette, *"Back to the Future: How Federal Courts Create a Federal Common Law Copyright Through Permanent Injunctions Protecting Future Works,"* 2 J. Intell. Prop. L. 325, 340 (1994)). However, since injunctions in non-copyright cases have frequently been held to be unconstitutional prior restraints on speech, *Near* v. *Minnesota*, 283 U.S. 697 (1931); *New York Times Co.* v. *United States*, 403 U.S. 713 (1971), and for other reasons, the subject has arisen as to the application, if any, of the First Amendment to copyright principles. *See generally*, Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 19 (2010).

The issue of whether and, if so, how certain elements of the Copyright Act should be read to accommodate various First Amendment interests remains open. The law could hardly be clearer, however, that injunctions are a longstanding, constitutionally sanctioned way to remedy and prevent copyright violations. Indeed, that premise was explicit in the critical concurring opinion in the Supreme Court's most famous prior restraint case, assessing publication of the Pentagon Papers, which noted that "no one denies that a newspaper can properly be enjoined from publishing the copyrighted works of another." *New York Times Co.*, 403 U.S. at 731 n.1 (White, J. and Stewart, J., concurring). Current treatises reflect this judicial consensus. "[C]ourts have found no constitutional obstacle to enjoining, pursuant to federal legislative mandate, the unlawful use of a registered trademark or copyright." Floyd Abrams & Gail Johnston, *Communications Law in the Digital Age 2010: Prior Restraints*, 1026 PLI/Pat 247, 261 (2010); James L. Oakes, *Copyrights and Copyremedies: Unfair Use and Injunctions*, 38 J. Copyright Soc'y 63, 71 (1990) ("A pirated or copied edition, record, movie, song or other work . . . cries out for an injunction").

The Supreme Court's most detailed treatment of the interrelationship between the First Amendment and copyright, the seminal case of *Harper & Row Publishers, Inc.* v. *Nation Enterpr.*, 471 U.S. 539, 560 (1985), stressed that far from conflicting with the First Amendment, the Copyright Act actually furthers the very interests which the First Amendment protects. "First Amendment protections," the Court noted, are "already embodied in the Copyright Act's distinctions

between copyrightable expression and uncopyrightable facts and ideas." The Constitution supports the explicit protection of such expression and creativity, the Court stated, within a framework that defends *both* the right to speak *and* the ability to profit from speech. "[T]he Framers intended copyright itself to be the engine of free expression," explained the Court, and "[b]y establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." *Id.* at 558. Copyright law thus fortifies protections for speakers and creators, in a First Amendment context, while stimulating future creativity.

The evident constitutionality of injunctive relief for copyright violations does not mean, to be sure, that injunctions must automatically or always be issued in response to a copyright violation, nor that the seizure powers under the copyright law must be exercised without due regard to First Amendment considerations. Indeed, the Supreme Court has cautioned against the error of making a "categorical grant" of injunctive relief for patent infringement in *eBay Inc.* v. *MercExchange, L.L.C.*, 547 U.S. 388, 394 (2006), a proposition of law that the Second Circuit applied in a recent, celebrated copyright case, *Salinger* v. *Colting*, 607 F.3d 68 (2d Cir. 2010). What *no* court has ever denied, however, is that injunctions are a valuable and constitutional response to copyright violations.

Legislative Summary

I turn to a discussion of the bill itself. The Stop Online Piracy Act is designed to enforce federal copyright and trademark law in the age of the Internet. Hearings before this Committee have powerfully revealed what Chairman Smith has aptly characterized as the "destructive effects of online 'parasites' -- web-based entities that steal intellectual property." The Stop Online Piracy Act aims to combat the theft and infringement of American intellectual property, copyrights and trademarks, whether such activity originates within or beyond the United States.

The bill does so by strengthening the measures that the Attorney General and private parties may pursue, with court approval, to address infringing content. The bill buttresses injunctive relief previously available against infringing websites by providing a mechanism to compel operators of domain name lookup services, payment network providers, Internet advertising services, and search engines to cease supporting or cooperating with foreign infringing websites.

Attorney General Actions Against Foreign Infringing Sites

The Stop Online Piracy Act aims to counter the copyright infringement of "foreign infringing sites," which it defines as sites that are (1) "committing or facilitating the commission of criminal violations" under current law,[2] (2) which would, based on those criminal violations, "be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site," and (3) which are directed at the U.S. and used within the U.S.

For these foreign infringing sites, the bill authorizes the Attorney General to commence two types of actions. The Attorney General may commence an in personam action against the registrant of a domain name used by a foreign infringing site, or an owner or operator of a foreign infringing site. If such an individual cannot be located "through due diligence" by the Attorney General, then an in rem action may be commenced against the foreign infringing site or the foreign domain name used by such site.

Upon commencing one of these actions, the Attorney General shall send a notice of alleged violations and intent to proceed to the registrant of the domain name of the site, via both email and postal mail addresses listed in the applicable public registration database, and via both email and postal mail addresses of the registrar, registry or other domain name registration authorities that registered the domain name at issue (to the extent available). Likewise, the Attorney General shall send the same notice to the owner or operator of the site, via both email and postal mail, or, if there is no domain name, to the IP allocation entity, via both email and postal mail, as well as notice to the site's owner or operator in any other form that a court "may provide," including as may be required by Rule 4(f) of the Federal Rules of Civil Procedure.

Under the bill, courts "may" issue a temporary restraining order, a preliminary injunction or an injunction "in accordance with rule 65 of the Federal Rules of Civil Procedure," against the site's operator, a registrant of a domain name used by the site, the site itself, or a "specified portion" of the site, to order that it "cease and desist from undertaking any further activity as a foreign infringing site."

By incorporating Rule 65, the bill applies the procedural protections that federal law currently affords all litigants in civil actions in the United States.

Under Rule 65, courts "may issue a preliminary injunction only on notice to the adverse party." For temporary restraining orders to be issued without notice, Rule 65 requires that two

---

2 The enumerated laws are sections 2318, 2319, 2319A, 2319B, 2320 or chapter 90 of title 18 U.S.C (counterfeit labels, criminal infringement of copyright, trafficking in counterfeit goods or services, unauthorized recordings of motion pictures, unauthorized trafficking in sound recordings and music videos, and trade secrets).

conditions must be met. "[S]pecific facts in an affidavit or verified complaint [must] clearly show that immediate and irreparable injury, loss, or damage will result . . . before the adverse party can be heard in opposition." And "the movant's attorney [must] certif[y] in writing any efforts made to give notice and the reasons why it should not be required." Hearings for orders without notice are to be held "at the earliest possible time, taking precedence over all other matters," under Rule 65, and the adverse party may move to dissolve or modify an order on two days' notice to the moving party. All these protections are incorporated into the legislation.

Pursuant to the Act, once court orders are issued, with "prior approval of the court," a process server on behalf of the Attorney General may serve a copy of a court order on four types of entities that may be cooperating with the site question. First, service providers shall "prevent access" by its U.S. subscribers "to the foreign infringing site (or portion thereof) from resolving to that domain name's [IP] address," and may display a notice informing visitors that the operator is taking an action pursuant to a court order. The text of this notice is to be prescribed by the Attorney General, and specify that the action is being taken pursuant to a court order. Second, search engines[3] shall prevent the site, or a specified portion of the site, from being served as a direct hypertext link. Third, payment network providers shall prevent, prohibit or suspend payment transactions between U.S. customers, or customers subject to the jurisdiction of the U.S., and the site. Fourth, Internet advertising services shall prevent their networks from providing advertisements to the website named in the order.

Each of these entities are to take "technically feasible and reasonable measures" to comply within five days of receiving an order. In the case of service providers, the Stop Online Piracy Act states such providers "shall not be required" to modify their network or facilities to comply with such orders; nor to take "measures with respect to domain name resolutions not performed by its own domain name server"; nor to continue taking preventive actions under the order once access to the domain name has been "effectively disabled by other means." The bill also notes that these enumerated protections do not "affect" or weaken the limitation on liability of such operators under section 512 of title 17 U.S.C.

The bill neither compels nor prohibits speech or communication by the four entities regarding any measures they take.[4] The entities may decide, at their discretion, "whether and how to communicate" their actions to users or customers.

---

[3] The bill provides an original definition for Internet search engines. Previous Senate bills sought to regulate search engines with reference to the statutory term "Information Location Tools," as defined in the Digital Millennium Copyright Act (DMCA) (section 512 of title 17 U.S.C.).

[4] The single possible exception to this description is the bill's provision that the Attorney General "shall prescribe the text of any notice displayed to users or customers of a service provider taking action pursuant to [the bill's remedies.]"

In the event of a willful and knowing failure to comply with orders under the bill, the Attorney General may seek injunctive relief directly against the entity in question. In such actions, technological inability to comply with the order "without incurring an unreasonable economic burden" shall serve as an affirmative defense. A showing that the order in question is not authorized under the Stop Online Piracy Act shall also serve as an affirmative defense. In addition, the bill does not limit or revoke current defenses to copyright infringement that may be offered, including but not limited to that of fair use. Entities taking actions reasonably designed to comply with court orders issued under bill are granted immunity from causes of action based on such compliance.

Qualifying Plaintiff Actions Against Sites Dedicated to the Theft of U.S. Property

In addition to the Attorney General's powers to pursue foreign infringing sites under the Stop Online Piracy Act, the bill also provides for a "market-based" system to address online infringement, including the establishment of a private right of action, in specified circumstances against sites "dedicated to the theft of U.S. property."

Under this approach, the above remedies may be sought by qualifying plaintiffs through, first, a cooperative notification process, and second, in the event of noncompliance or dispute, by commencing an action against infringing sites and, with court approval, serving orders on payment network providers and Internet advertising services. This private right of action accorded to these third party entities is limited in scope. It does not provide for serving orders on service providers or search engines. The private right of action includes the same protections of Rule 65, the prioritization of in personam actions against U.S. individuals over in rem actions against domains, and the same requirements regarding notice, service of process and domain activity within the U.S.

This part of the Stop Online Piracy Act applies to sites, or specific portions of sites that are "dedicated to the theft of U.S. property" and directed towards the U.S., used by people in the U.S., and which are either (1) primarily designed or operated for the purpose of, or have only limited purposes other than, offering goods or services in violation of, or facilitating the violation of, current copyright or trademark law; or (2) the site operator is taking actions to "avoid confirming a high probability of the use of the site or portion thereof" is in violation of copyright and trademark law, or the individual operates the site or a portion thereof to promote its use to carry out violations of copyright and trademark law.

The qualifying plaintiffs are rights-holders of the intellectual property at issue. Before commencing any action in court, however, these plaintiffs must follow a formal notification process regarding any alleged sites dedicated to the theft of U.S. property. Plaintiffs must provide a written, signed communication to the designated agents of the two entities governed under this provision, financial service providers and Internet advertising services, which identifies the site and provides a statement and specific facts supporting the claim (under penalty of perjury), with facts establishing that the entity is servicing the site. Such a notification shall trigger private action remedies by the entity to cease their services for the site, unless the site owner or operator provides a counter-

notification to the entities disputing the claims, under penalty of perjury, and consenting to jurisdiction of U.S. courts.

In the event of a counter-notification or a failure by the entities to comply with the initial notification request, a qualifying plaintiff may commence an in personam action against the operator or owner of the site, or the registrant of the domain name. If a qualifying plaintiff, authorized under these conditions to bring such an in personam action, cannot "find a person" affiliated with the site to sue after due diligence, or no such person has an address in the U.S., the bill enables the plaintiff to commence an in rem action against the site or domain name. The plaintiff must give notice, via email and postal mail, to the registrant, the site owner or operator, or the IP allocation entity if there is no domain name, as well as any other form of notice that a court may prescribe, including as required by rule 4(f) of the Federal Rules of Civil Procedure. Then, in a companion structure to the Attorney General actions outlined above, a court may issue a temporary restraining order, preliminary injunction or injunction "in accordance with rule 65" against a registrant or site operator, and with prior approval of the court, such orders may be served on payment network providers and advertising services.

First Amendment Considerations

Having discussed the broad constitutional and copyright framework for the Stop Online Piracy Act, and described what the bill does in basic terms, I now turn to two potential First Amendment issues in analyzing this legislation: the procedural protections in a First Amendment context, and issues related to potential overbreadth of the bill.

Procedural Protections

The Stop Online Piracy Act's procedural protections are so strong, uniform and constitutionally rooted that it is no exaggeration to observe that complaints in this area seem not to really be with the bill, but with the Federal Rules of Civil Procedure itself, which govern all litigants in U.S. federal courts.

For potential suits by both the Attorney General and qualifying private party plaintiffs, the bill incorporates Rule 65 to provide the process governing how a judge "may" issue a temporary restraining order, preliminary injunction, or injunction. Thus website operators subject to the bill, including foreigners, would benefit from the same procedural safeguards afforded litigants in all other U.S. civil actions. For preliminary injunctions, those safeguards require notice in advance. For temporary restraining orders, the safeguards include first, the requirement that temporary restraining orders issued without notice must be based on specific facts showing the prospect of immediate and irreparable damage "*before* the adverse party can be heard in opposition" (emphasis added); and second, a written certification by the attorney (for the government or the plaintiff, depending on the action), explaining efforts made to give notice and the reasons it should not be required in this instance. Subsequent hearings for orders without notice are a first priority under Rule

65, which also grants the adverse party the option of moving to dissolve an order with two days' notice.

In addition to those well-established procedures, the bill requires several measures to ensure due process. First, the Attorney General or qualifying plaintiff must commence an in personam action against the registrant, owner or operator of a website dedicated to infringing activities, if it is possible to locate such an individual through due diligence. This approach, (which provides an additional step compared to the Senate's COICA legislation), may provide more warning and the prospect of adversarial hearings before injunctive relief -- at least in situations where such an individual resides in the U.S. and has provided accurate contact information. For in rem actions, the bill explicitly requires service of process by sending notice of the alleged violation and intent to proceed to the registrant, by email and postal mail listed in a public database, by email and postal mail of the registrar, as well as in any form a court finds necessary under Rule 4(f) of the FRCP. Consistent with the objectives of Rule 65, this requirement provides an opportunity to operators of allegedly infringing websites to defend themselves before an order is issued.

In the event that operators choose to respond later, or only learn of injunctive action later because they did not provide accurate contact information to their registry, they still retain their rights to seek later relief from the order by disputing the allegations or appealing to the interests of justice.[5] It is worth noting, in addition, that federal copyright law disfavors the submission of false contact information to a domain name registrar, treating the knowing provision of "materially false contact information to a domain name registrar" as a rebuttable presumption of willful infringement. 17 U.S.C.A § 504(c); *Chanel, Inc.* v. *Cui*, 2010 WL 2835749 (S.D.N.Y. July 7, 2010) (entering default judgment for permanent injunction against product trademark infringement and finding willful conduct based, in part, on defendant's repeated submissions of "false information in registering domain names" used for infringement). Finally, since the bill states that courts "may" issue preliminary injunctions or injunctions, the range of available remedies includes the prospect of a final—not preliminary—resolution of the dispute.

Even when the Stop Online Piracy Act's required procedural protections are satisfied, some operators of allegedly infringing websites may knowingly decline to participate in U.S. court proceedings. Such a choice, after legitimate notice and procedural safeguards are provided, may lead to *ex parte* proceedings and default judgments. Courts routinely enter default judgments in civil lawsuits, including comparable online copyright cases. After initial notice has been served, courts grant permanent injunctive relief for copyright violations in default judgments without additional attempts at notice. *Disney Enterprises, Inc.* v. *Farmer*, 427 F.Supp. 2d 807 (E.D. Tenn. 2006) (issu-

---

[5] Each of these protections applies regardless of whether the Attorney General or a qualifying plaintiff commences an action. While the prospect of potential actions by private plaintiffs, which was not authorized by the COICA legislation, is one which raises significant policy issues, it does not fundamentally alter First Amendment and due process analysis in this area.

ing permanent injunction barring infringement of copyright by website distributing copyrighted movies over peer-to-peer network, with default judgment entitled without additional service of notice on defendant); *Priority Records, LLC* v. *Bradley*, 2007 WL 465754 (E.D. Mich. Feb. 8, 2007) (issuing permanent injunction in default judgment against defendant using online distribution system to download and distribute copyrighted recordings).

Breadth and Precedent

It is a fundamental principle of First Amendment jurisprudence that government restrictions on speech should be narrowly tailored to avoid unnecessarily burdening protected speech. Courts closely scrutinize statutes that may hinder protected speech, and give special attention to rules that could sweep too broadly. As with any statute impacting speech, Congress must consider the potential overbreadth of the Stop Online Piracy Act's regulatory structure, both in how it is drafted and how it should be applied, in light of such First Amendment considerations.

Recent Senate bills in this area, COICA and the Protect IP Act, sought to address such First Amendment concerns, in part, by defining a statutory definition for the type of websites so predominantly engaged in infringement that orders to block, thwart or deter such activities would not have an excessive or unnecessary impact on protected speech.[6] As a trigger, the Protect IP Act effectively required that sites had no significant use other than infringement, or were designed, operated or marketed primarily for infringement. COICA provided a similar trigger in its definition for sites dedicated to infringing activity, and in addition, it provided an alternative definition based simply on the government's civil forfeiture powers under current law. Therefore, apart from any references to current law, both bills sought to define, in specific statutory language, something akin to a minimum threshold for triggering these new remedies to counter infringing sites.

The Stop Online Piracy Act does not articulate such a standard for actions by the Attorney General.[7] Instead, it cites to and is rooted in current copyright, trademark and seizure law,

---

[6] The standard would be relatively new for a federal statute, although it is worth noting that the framework of sites "dedicated to infringing activities" was based on a precedent for online infringement liability in *Metro-Goldwyn-Mayer Studios Inc.* v. *Grokster, Ltd.*, 545 U.S. 913, 936 (2005).

[7] The bill does define a term for sites "dedicated to theft of U.S. property" in its section on actions by qualifying plaintiffs, but my First Amendment analysis begins and focuses on the bill's earlier provisions regarding actions authorized only for the Attorney General, which reflect the strongest remedies provided for in the legislation.

similarly to the alternative definition in COICA, so as to extend the Attorney General's authority to foreign infringing sites and provide for remedies against third party intermediaries.[8]

The Stop Online Piracy Act uses three tests to define foreign infringing sites: First, the site must be committing or facilitating criminal violations of copyright or trademark law; second, those violations must "be subject to seizure" in the U.S. "if such a site were a domestic Internet site"; and third, the site (or portion thereof) must be directed at the U.S. and used within the U.S. The bill incorporates this seizure standard for definition purposes only -- it does not initiate the entire procedure of the forfeiture laws, nor does it trigger an actual forfeiture. Instead, as discussed above, the Stop Online Piracy Act enumerates its own set of procedures, consistent with Rule 65 and including enumerated notice requirements, and sets forth its own remedies against foreign infringing sites. Those remedies include injunctive relief ordering sites to cease violating the law, and serving orders, with court approval, on the four enumerated intermediaries. In contrast to the civil forfeiture procedures, these remedies are weighed under the traditional standards for injunctive relief.

In recent cases, courts have issued seizure warrants against domain names based on a probable cause finding of infringement, which can result in orders on registries to lock and seize domain names. *United States* v. *TVShack.net et al.*, 2010 WL 2666284 (S.D.N.Y. June 29, 2010) (treating domain names hosting infringing videos as forfeitable property under 18 U.S.C. §§ 2323(a) and ordering their seizure). There is a challenge to that domain name seizure process, on both statutory and First Amendment grounds, currently pending in the Second Circuit. In *Puerto 80 Projects* v. *United States*, the United States Southern District Court of New York rejected a challenge by operators of a Spanish website to the government seizure of its domain names, finding the loss of the domain names at issue did not constitute a substantial hardship under the law, but the court noted that First Amendment issues could still be argued on a future motion to dismiss.[9] (The Second Circuit is scheduled to hear argument in the case in December 2011.) If the Stop Online Piracy Act were adopted and courts ultimately alter, narrow or restrict the current application of the seizure standard to domain names, whether on First Amendment grounds or for other reasons, the Stop Online Piracy Act would incorporate the new standard. In other words, if the courts hold that the First Amendment demands a higher standard than is currently applied for seizure of domestic property implicating protected speech, the Stop Online Piracy Act would automatically import such a standard, given its definition trigger referencing sites "subject to seizure" in the U.S.

Regardless of the particular standard or definition of foreign infringing sites, court-approved remedies under the Stop Online Piracy Act may result in the blockage or disruption of

---

[8] The definition refers to sites "committing or facilitating the commission of criminal violations" under current law, which would, based on those criminal violations, "be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site."

[9] No. 11 Civ. 4139 (S.D.N.Y. Aug. 4, 2011).

some protected speech. As discussed above, the bill provides a range of injunctive relief is available, with a court making the final determination as to whether and how to craft relief against a website operator or owner or third party intermediaries. When injunctive relief includes blocking domain names, the blockage of non-infringing or protected content may result. The presence of some non-infringing speech, in and of itself, generally does not provide a copyright violator with immunity from enforcement actions under current caselaw. The First Amendment allows government regulations to prevent piracy that has an incidental impact on non-infringing speech. *United States* v. *Elcom Ltd.*, 203 F. Supp. 2d 1111, 1129 (N.D. Cal. 2002) (noting that the First Amendment allows the government to pursue online infringement with an "incidental restriction" on First Amendment freedoms, so long as the traditional test is met that the "means chosen do not burden substantially more speech than is necessary to further the government's legitimate interests") (internal citations omitted). If an order under the bill does result in blocking some non-infringing content, the bill is sufficiently narrow to accommodate the immediate publication of that content elsewhere and the future publication of the content on the same domain. First, by definition, any non-infringing content is not specifically enjoined by the order, so it may still be legally posted anywhere else online. Second, such content may be unblocked or reposted *on the same* website or domain name in the future, once the infringing content at issue is removed. After the infringement issue is resolved and the site operator is in compliance with federal law, the domain name may post its archived non-infringing content.

Finally, it is worth noting that legislation in this area typically implicates linking, a key part of the Internet's architecture, in two ways. Sites may facilitate infringement by linking alone, without directly hosting infringing content, and the Stop Online Piracy Act's remedies include potential injunctions against linking by search engines, pursuant to a court order. These measures' impact on linking are not overbroad, nor a break from precedent.

In recent enforcement actions against domain names, the U.S. Department of Homeland Security has seized "'linking' websites" which provided "links to files on third party websites that contain illegal copies of copyrighted contact." (Aff. ¶ 13) *United States* v. *The Following Domain Names: HQ-Streams.com et al.*, 2011 WL 320195 (S.D.N.Y. Jan 31, 2011). Targeting such linking is also consistent with caselaw regarding online copyright infringement, since "[l]inking to infringing material" can create secondary liability, 1003 PLI/Pat 35 at 43. Under current law, when a website links to infringing content, or links to technology to facilitate infringement, courts look to whether the website operator knowingly linked to facilitate violations of the law. *Universal City Studios, Inc.* v. *Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (holding defendant violated DMCA by linking to program to unlock DVDs for unauthorized copying, and requiring knowing linking for the purpose of disseminating the program, and holding that prohibiting technology designed to circumvent protections for copyrighted works did not violate the First Amendment); *Bernstein* v. *JC Penney, Inc.*, 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998) (plaintiff did not have a claim for mere linking to website without knowledge of infringing material on the site). With regard to potential injunctions against search engine linking -- a situation where there may be no knowledge element, and thus no secondary liability -- courts still retain the authority to issue injunctive relief specifically against linking, as a means to remedy ongoing or potential copyright infringement. *Universal City Studios,*

Inc. v. *Corley*, 273 F.3d 429 (2d Cir. 2001) (holding that injunctions issued against linking to thwart copyright infringement was consistent with the First Amendment). Even in cases that have narrowed injunctions against linking based on First Amendment violations regarding overbreadth, protected criticism and noncommercial speech, courts have still upheld injunctions tailored to protect intellectual property rights by barring commercial links. *Nissan Motor Co.* v. *Nissan Computer Corporation*, 378 F.3d 1002 (9th Cir. 2004) (holding injunction violated First Amendment "to the extent that it enjoins the placing of links [] to sites with disparaging comments" about plaintiff's business, but upholding injunction compelling defendant to "refrain from displaying" links about the plaintiffs' business on website with similar name, and holding trademark was infringed by certain links).

Given these precedents, actions against websites (or a portion thereof) committing violations by linking, not hosting, appear to rest on a solid constitutional foundation; potential injunctions against linking to such sites, pursuant to a court order, are consistent with courts' current remedies for intellectual property violations online.

Conclusion

Any legislative efforts to limit what appears on the Internet, or to punish those who post materials on it, requires the closest scrutiny to assure that First Amendment rights are not being compromised. That is true of all limits on speech, and it is no less true of the Internet. But the Internet neither creates nor exists in a law-free zone, and copyright violations on the Internet are no more protected than they are elsewhere.

The notion that adopting legislation to combat the theft of intellectual property on the Internet threatens freedom of expression and would facilitate, as one member of the House of Representatives recently put it, "the end of the Internet as we know it," is thus insupportable. Copyright violations have never been protected by the First Amendment and have been routinely punished wherever they occur, including the Internet. This proposed legislation is not inconsistent with the First Amendment; it would protect creators of speech, as Congress has done since this Nation was founded, by combating its theft.

Respectfully submitted,

Floyd Abrams*

* I thank my associate and colleague, Ari Melber, for his assistance in all aspects of the preparation of this submission.

Mr. SMITH. Thank you, Mr. Conyers.

The gentleman from Virginia, Mr. Goodlatte, the Chairman of the Intellectual Property Subcommittee, is recognized.

Mr. GOODLATTE. Mr. Chairman, thank you for holding this hearing, and thank you for your leadership on this issue.

For more than two centuries, America's economic strength has been built on a firm foundation. The rule of law, respect for individuals and private property, and the promotion of industry through policies that reward creativity and innovation are essential virtues that helped the fledgling Nation encourage the initiative of its citizens, and in time emerged the most advanced and prosperous on earth. These virtues are not universal. In an increasingly connected world, threats that emanate from areas where these principles are not shared are jeopardizing our ability to sustain the

incentives needed to foster growth and development and advance human progress.

These threats create challenges for us in both the physical world and the virtual world where the systematic and willful violation of intellectual property rights now poses a clear, present, and growing danger to American creators and innovators, U.S. consumers, and our collective confidence in the Internet ecosystem.

In order to continue to incentivize artists, authors, and inventors, we need to ensure that these creators have the ability to earn a return on their investments. Increasingly, foreign piracy is stripping creators of that ability. Within the Internet ecosystem today, there are legitimate commercial sites that offer consumers authorized goods and services. Indeed, many exciting new technologies and websites help content owners distribute music, movies, books, games, software, and other copyrighted works in ways that were not even imaginable 10 years ago. However, there are also rogue sites that steal the intellectual property of others, and traffic in counterfeit and pirated goods.

In recent years, these websites have grown and evolved. They have become increasingly sophisticated and rival the legitimate sites in appearance, operation, and indicia of reliability.

U.S. consumers are frequently led to these sites by search engines that list them among the top search results. After clicking on a site, they are immediately reassured by the logos of U.S. payment processors and the presidents of major corporate advertising supporting the site. These sites sell infringing copyrighted works, but they are not limited to those. Increasingly, these sites also offer counterfeit goods, such as counterfeit automobile parts, medicines, baby formula, and other products that can pose serious threats to the health and safety of American citizens. What is worse, these rogue sites often list the real customer service contact information for the legitimate companies, which deteriorates the reputation of the legitimate maker of these goods.

For all these reasons, I have joined Chairman Smith in introducing the Stop Online Piracy Act, which creates new tools for law enforcement to combat these growing threats. Specifically, this legislation gives law enforcement the authority to bring an action in a Federal court to declare a website in violation of the law, and allows the court to issue a court order to intermediaries to block transactions and access to those sites found to be infringing. The bill also provides content owners with a limited liability to request a court to declare a website as violating the law. However, the content owners must first attempt to work directly with financial services and advertising intermediaries to solve the problem. Only if those parties cannot reach agreement are content owners allowed to seek a court declaration against and infringing website.

It is my hope that this provision will allow content owners and intermediaries to work together to root out infringing sites quickly.

It should be noted that there has been criticism from many in the online community about the scope of this bill, its effect on the functioning of the Internet, and that it could entangle legitimate websites. It is not my intention to do so, and I stand ready to work with the tech community to address any legitimate concerns they have. I have requested detailed comments from the tech community

about their concerns, and look forward to continuing to work with them and Chairman Smith and other Members of the Judiciary Committee to ensure that this legislation punishes lawbreakers while protecting content owners as well as legitimate online innovators and startups.

Mr. Chairman, this is a good bill, but a number of issues raised about it need to be carefully addressed. I look forward to working with you on those issues as we move forward to protect content owners online, and I look forward to hearing from our witnesses today.

Mr. SMITH. Thank you, Mr. Goodlatte.

The gentleman from North Carolina, Mr. Watt, the Ranking Member of the Intellectual Property Subcommittee, is recognized.

Mr. WATT. Thank you, Mr. Chairman.

Mr. Chairman, in my experience, there is usually only one thing that is at stake when we have long lines outside a hearing, as we do today, and when giant companies, like those opposing this bill and their supporters, start throwing around rhetoric like, "This bill will kill the Internet," or, "It is an attempt to build the great firewall of America." And that one thing is usually money.

While I appreciate that the stakeholders of Internet companies that have market caps in the billions of dollars care, as we all do, about the First Amendment and other precious rights, it seems clear to me that the obstinate opposition we have seen in the days since introduction of the Stop Online Piracy Act is really about the bottom line—piracy and counterfeiting, make money, and lots of it.

This is not speculative. Sites that specialize in stolen goods attract a lot of eyeballs, which, in turn, attracts a lot of advertising, which in turn means, well, you got it, lots of money.

To be fair, many of the copyright and trademark owners who want this bill to help enforce their rights are also businesses owners and are also motivated by money. But in my mind, stopping theft of your work or products is an appropriate incentive to secure profits. But doing nothing or next to nothing to prevent theft through the use of tools a company creates or controls is not an appropriate incentive to secure profits.

So, as policymakers, our goal must be to confront the criminal enterprises that are flourishing on the Internet, stealing from the rightsholders, and visiting untold harm on consumers. Doing nothing is not an option. Not only are online piracy and counterfeiting drains on our economy, they expose unworried consumers to fraud, identity theft, confusion, and, at worst, physical harm. The penetration of hazardous product and goods into the American marketplace, including our military supply chain, poses an unacceptable risk of serious bodily injury or death to our citizens. Tolerance of online theft of music, movies, and software reinforces a culture of entitlement, stifles creativity, injures artist, and undermines job stability and growth.

While I have never been a big advocate of current seizure laws, why would we not, as this bill does, give the Attorney General, at a minimum, the same power to block foreign thieves from access to the U.S. markets as the Attorney General has for domestic markets? Given the limits of government resources, why should we not establish a framework to enable rightsholders to engage specific

intermediaries within the Internet ecosystem to meet the challenges of online piracy and counterfeiting?

I think one of the big problems here is that to date, the economic incentives for the big Internet companies to work against online piracy are just not there. To be sure, there are many intermediaries that are inadvertently involved with pirate sites who have come to the table with constructive suggestions for crafting a balanced bill that will work. I commend ISPs, payment processors, like MasterCard, who is here today, and Visa, Go Daddy, who is the largest registrar of domain names, and a number of software companies who have raised reasonable concerns, and are willing to work together to address them. But, again, when I hear overblown claims like, this bill is a "Give away to greedy trial lawyers," or "A killer of innovation and entrepreneurs," that the co-sponsors of this bill are the "Internet killers," I become suspicious of the message, as well as the messengers.

As is and as one who cares deeply about the constitutional guarantees of free speech and due process, it is beyond troubling to hear hyperbolic charges that this bill will open the floodgates to government censorship. That is simply not the world we live in, and to suggest that by establishing a means to combat theft of intellectual property online, we will somehow default into a repressive regime, belittles the circumstances under which true victims of tyrannical government actually live.

I urge everyone to set aside all the hyperbole and accusations. I am the first to admit that I do not like or love everything about this bill, but it is a very strong, solid effort to begin the process of responsibly providing the Attorney General and rightsholders with necessary tools to keep pace with, and ultimately, to outpace the high-tech bandits roving the Internet. I believe there are still some things we can do in the legislation to avoid unintended consequences, maintain the integrity of the Internet, and preserve certain freedoms, including many of the specific suggestions made by the Ranking Member.

Our staffs have worked closely together to identify ways to improve this bill, and we will continue to do so. And I appreciate the fact that crafting a bill governing the online environment requires attention to technological details. But I start from the premise that Internet freedom does not and cannot mean Internet lawlessness, and that the goals of freedom and lawfulness are no more incompatible in the Internet space than they are in the physical world.

Mr. Chairman, there is an African proverb that says, when elephants fight, it is the grass that suffers. Perhaps if we refocus this debate on the ills that may befall innocent consumers who fall prey to the perils of pirated and counterfeit goods rather than on the balance sheet of all the big companies, we can reach a worthy compromise.

I look forward to hearing from the witnesses, and engaging in ongoing dialogue as we move the bill forward. The stakes for America and American consumers are too high to get engaged in too much hyperbole.

Mr. Chairman, I yield back the balance of my time.

Mr. SMITH. Thank you, Mr. Watt.

Without objection, other Members' opening statements will be made a part of the record.

[The prepared statement of Mr. Forbes follows:]

Opening Statement of Representative J. Randy Forbes
House Judiciary Committee Hearing on
H.R 3261, the "Stop Online Piracy Act"
November 16, 2011

Mr. Chairman, targeting rogue websites to combat piracy and to protect intellectual property is a laudable goal. Our ability to protect the intellectual property of American entrepreneurs, inventors, and authors is critical to our nation's economic success. Profitable American businesses and ventures result in jobs for our citizens. At the same time, when profits are lost to counterfeit goods being sold at lower costs on rogue websites, businesses are forced to reduce the size of their workforce.

In an effort to ensure that all interested parties have the opportunity to be heard on this legislation, I would like to submit a statement attributed to Jordan Sekulow, Executive Director of the American Center for Law & Justice: "Online piracy is a real problem, specifically by web sites and actors located overseas. The latest move by Congress to address the problem is the Stop Online Piracy Act (H.R.3261). Unfortunately, as drafted, SOPA presents serious free speech and free press concerns, and would allow the First Amendment rights of innocent, uninvolved Americans to be curtailed. Authorizing private parties, for example, to limit and censor Internet service providers and web sites that access to the World Wide Web where pirated material is available, is like shooting an ant with an elephant gun. Before moving to approve any legislation on this issue, Congress would be well-served to go back to the drawing board and write a much more narrowly-tailored bill that reaches only the bad actors and offending parties."

Mr. Chairman, I look forward to working with Members of this Committee to protect the intellectual property of our citizens in a manner that does not infringe on the constitutionally protected rights on American businesses.

[The prepared statement of Ms. Lofgren follows:]

Congresswoman Zoe Lofgren
Opening Statement for the Record
Committee on the Judiciary
Hearing on H.R. 3261, the Stop Online Piracy Act
November 16, 2011

The matter before us today is enormously important. H.R. 3261, the Stop Online Piracy Act, would reshape our country's legal framework for online innovation and commerce, and perhaps the technical structure of the global Internet as well.

Unfortunately, the panel of witnesses convened for this hearing is severely inadequate. Civil libertarians and law professors have said this bill is inconsistent with the First Amendment to the United States Constitution. Network engineers and security experts have said that the bill could imperil cybersecurity and the technical infrastructure of the Internet. Consumer groups have expressed worries that the bill could raise the prices we pay for goods online. Human rights advocates have said that the bill could legitimize Internet censorship by repressive regimes around the world. Libraries and educational institutions have expressed concern that they could face new criminal and civil liability for innocent conduct. Venture capitalists and technology entrepreneurs have said that H.R. 3261 could stifle investment in legitimate Internet businesses and online services.

None of these voices are represented at our hearing today. Members will not have the opportunity to explore any of these concerns in detail. In their place, a single Internet company—Google—was invited to testify, on a panel with five other witnesses testifying in defense of H.R. 3261.

Infringing material exists on the Internet. Some websites exist that flagrantly violate copyright and trademark law. The question is what to do about it. No one should conflate opposition to this legislation with a disregard for the protection of intellectual property. Yet this is precisely what many of this bill's proponents are doing, in an attempt to discredit substantive criticisms. H.R. 3261 is deeply flawed in many ways. I will highlight just a few:

- Section 102 creates an open-ended technical mandate on Internet service providers (ISPs) to block their users from accessing blacklisted websites. Unlike S. 968, the PROTECT IP Act, this mandate is not limited to domain filtering. Instead, the government may apply for a court order to impose any filtering measure upon ISPs, so long as it is deemed "technically feasible and reasonable." Does this include the blocking Internet Protocol addresses? Deep packet inspection? New filtering technologies as they are invented? The bill does not say.

- Section 103 overturns critical safeguards in the Digital Millennium Copyright Act for cloud computing and any website that provides a platform for user-generated content. This includes everything from photo and video sharing to social networking, blogging, and beyond. Under Section 103, such websites will face a new legal risk that they will be

terminated by their payment and advertising providers, based on an accusation that they are dedicated "to the theft of U.S. property." This charge could be based upon infringement committed by a website's users, and the DMCA safe harbor in 17 U.S.C. 512(c) cannot be used as a defense.

- Section 103 also allows a "portion of" a website to be deemed "dedicated to the theft of U.S. property," regardless of the culpability of the website as a whole. Like many important terms throughout H.R. 3261, the precise meaning of these words is ambiguous, and will require years of expensive litigation to clarify. However, the plain meaning of the words seems to indicate that any large website could face a risk of termination by payment and advertising providers based solely upon infringing material contained in a single web page.

- Under Section 103, any website, foreign or domestic, can be declared "dedicated to theft of U.S. property" if it takes "deliberate actions to avoid confirming a high probability of the use" of the site to carry out infringement. This appears to create a new basis for infringement liability in U.S. copyright law, which will take years and perhaps decades of difficult litigation to sort out. It also may impose a duty upon websites to monitor all user-generated content on their sites, in order to guard against a risk that their failure to do so would be construed as an act of "willful blindness." For many legitimate websites, active monitoring is simply not feasible, given the enormous volume of content uploaded by their users during every hour of the day.

Let me also add that the domain filtering scheme envisioned by H.R. 3261 will not be effective. Anyone determined to reach a blocked site may do so easily, merely by typing in the website's IP address into the navigation of their browser bar, instead of the site's domain name. Any ten year old could do it. Under this bill, the United States would construct an unprecedented Internet filtering scheme to block foreign websites. This is likely to have major costs and unintended consequences, while doing little to achieve the laudable goal of reducing online piracy.

I agree with the goal of fighting online copyright infringement. Narrowly targeted legislation that does not ensnare legitimate websites or undermine the Internet's technical and security infrastructure should be pursued. In particular, I believe that new remedies could deprive criminal websites of the revenues that motivate and enable their very existence, without doing unnecessary collateral damage. I also believe that a consensus on this issue between the content and technology industries is achievable. Unfortunately, H.R. 3261 is a draconian and one-sided approach that pushes us much farther away from such a consensus, instead of building towards it.

[The prepared statement of Mr. Johnson follows:]

December 11, 2011

Congressman Henry C. "Hank" Johnson, Jr.

Statement for the Record Re: Hearing on H.R. 3261, the Stop Online Piracy Act (SOPA)

I thank Chairman Smith for holding this hearing on H.R. 3261, the Stop Online Piracy Act of 2011 (SOPA). I support the goal of providing the Department of Justice (DOJ) with additional enforcement tools to combat foreign rogue websites. Piracy hurts everyone, both the companies who make content and products and those that distribute it in new and innovative ways. We must work to stop piracy, but must tread cautiously as we do not want to destroy the foundation upon which our entrepreneurs and artists create platforms of innovation.

I agree that we need to protect American innovation and fight online copyright infringement. Intellectual property-intensive industries drive America's economy and piracy does not benefit our American inventors or the American public. Consumers should not be harmed by counterfeit goods, such as substandard prescription drugs or other dangerous and defective products sold on counterfeiting sites.

At the hearing, the technology industry and payment processors identified some legitimate concerns with SOPA. Further, public interest and civil rights groups such as the American Civil Liberties Union, the Consumers Union, and the Consumer Federation of America, have expressed concerns about this legislation. Too many interested parties have concerns about SOPA that should not be ignored. I, however, do believe that there is a compromise that could be reached between the content, technology industries, and those groups representing consumer interests. Thus, at this time, I have some concerns with the legislation in its current form and firmly urge the Committee to consider any unintended consequences SOPA may cause before it marks up this legislation.

The Digital Millennium Copyright Act and Section 230 of the Communications Decency Act represent the legal underpinning of the view that intermediaries need not monitor or supervise the communications of users. It is a view that we have long touted and pushed across the world through various diplomatic channels. As some technology and public interest groups have pointed out, we have harshly criticized governments who use such virtual walls to prevent citizen access to the Internet. With that in mind, we must consider whether this legislation would allow companies to demand that search engines located inside of the United States censor

where American consumers are able to go on the Internet. We must consider how this legislation would be viewed by China, Iran, and other countries that have used some of the same actions required in SOPA to block speech. We must ensure that this legislation does not dampen diplomatic efforts on that front.

I also share concerns with the Library Copyright Alliance about the willfulness standard under the bill. Section 506 of the Copyright Act establishes criminal liability for the willful infringement of a copyright. My concern is that SOPA's rule of construction creates a negative implication that a person is a willful infringer if the person did not have a good faith reasonable basis in law for believing that his conduct was lawful. According to the Library Copyright Alliance, if a court finds that the person's belief was unreasonable, the court might consider him a willful infringer, even if the person in good faith believed his actions were legal. Under current law, however, this level of intent constitutes ordinary infringement, not willful infringement. This should be cleared up in SOPA before it moves forward.

With regards to payment processors, SOPA requires them to suspend payment transactions between a U.S. customer and an online merchant within 5 days after being served with a copy of an order or receiving notice from a private rights holder that a site is dedicated to the theft of U.S. property. At the hearing, MasterCard noted that there are many instances where a five-day window to suspend payment transactions may not be feasible. We should revisit this provision and work with the payment processors on identifying a reasonable amount of time before moving this legislation to the floor.

Finally, the DOJ is charged with more responsibility because SOPA grants it new enforcement tools to prosecute foreign rogue websites. With the DOJ taking budget cuts and downsizing antitrust units, including in my home state of Georgia, we must ensure that it has the resources and attorneys it needs to adequately prosecute foreign rogue sites under the bill.

As I stated earlier, piracy does not benefit our American inventors or the American public. I look forward to working with the Committee on these issues as I would support fine-tuned legislation that balances the need to combat piracy, foster innovation and would not entangle legitimate websites in the process.

Mr. SMITH. We welcome our distinguished panel today, and I will now introduce them.

Our first witness is Marie Pallante, the Register of Copyrights. Ms. Pallante was appointed by the Librarian of Congress, Dr. James Billington, as the 12th Register on June 1st of this year. Immediately prior to that appointment, Ms. Pallante served as the Acting Register.

As a Register, Ms. Pallante continues the tradition of serving as the principal advisor to Congress on matters of copyright policy. Ms. Pallante has spent much of her career in the office, where she previously served as the associate Register for Policy and International Affairs, Deputy General Counsel, and Policy Advisor. In addition, Ms. Pallante spent nearly a decade as Intellectual Property Counsel and Director of Licensing for the Guggenheim Museum in New York.

She earned her law degree from George Washington University and her Bachelor's degree from Misericordia University, where she was also awarded an honorary degree of humane letters.

Our second witness is John P Clark, the Vice President of Global Security and Chief Security Officer for Pfizer. Since joining Pfizer in 2008, Mr. Clark has been recognized as the leading authority on the threat that counterfeit medicines pose to patient health and safety.

Prior to joining Pfizer, Mr. Clark served as Deputy Assistant Secretary of the U.S. Immigration and Customs Enforcement. In that capacity he was responsible for overall management and coordination of the agency's operation, and he served as the Assistant Secretary's principal representative to the Department of Homeland Security and to the law enforcement and intelligence communities.

Starting as a U.S. Border Patrol Agent in 1980, Mr. Clark spent more than 25 years as a law enforcement professional before retiring from public service. A New York native, Mr. Clark received his Bachelor of Science degree in History from the State University of New York at Binghamton, and a Master of science degree from National-Louis University.

Our third witness is Michael O'Leary, the Senior Executive Vice President for Global Policy and External Affairs at the Motion Picture Association of America. In that position, Mr. O'Leary supervises all international, Federal, and State affairs operations around the world for the association.

Before moving to MPAA, Mr. O'Leary served more than a dozen years at the Department of Justice, where he worked on legislative, intellectual property, and enforcement issues. During his tenure at the DoJ, he served as the Deputy Chief of the Computer Crime and Intellectual Property section, where he prosecuted and supervised some of the most significant domestic and international criminal and IP cases undertaken by the Department. Before joining DoJ, Mr. O'Leary spent 5 years serving as Counsel to the Senate Judiciary Committee.

He grew up in Montana as a graduate of Arizona State University and the University of Arizona School of Law.

Our fourth witness is Ms. Linda Kirkpatrick, who serves as the Group Head of Customer Performance Integrity at MasterCard Worldwide. In this role, Ms. Kirkpatrick is responsible for driving

the strategy, development, and execution of global customer compliance programs, data integrity, and dispute resolution management.

Ms. Kirkpatrick has been with MasterCard since 1997. She earned her Bachelor of Arts degree in Economics with a concentration in Finance from Manhattanville College in Purchase, New York.

Our fifth witness is Katherine Oyama, a Policy Counsel for Google, where she focuses on copyright and trademark law and policy.

From 2009 to early 2011, she worked in the Office of the Vice President as Associate Counsel and Deputy Counsel to Vice President Joseph R Biden. Prior to her government service, Ms. Oyama was a litigation associate with Wilmer Cutler Pickering Hale & Dorr, where she worked on intellectual property cases, government regulatory, litigation, and pro bono matters. She previously worked in the Media and Entertainment practice of a New York-based strategy consulting firm, for the Silicon Valley-based Internet start-up, LoudCloud, Inc., and for a Texas-based company, Electronic Data Systems.

Ms. Oyama is a graduate of Smith College, where she graduated with honors in Government, and the University of California Berkeley School of Law, where she served as senior articles editor of the Berkeley Technology Law Journal.

Our final witness is Paul Almeida, the President of the Department for Professional Employees of the AFL-CIO.

Mr. Almeida has served as President of the DPE since February 2001. Prior to his tenure with DPE, Mr. Almeida served as President of the International Federation of Professional and Technical Engineers for 7 years.

Mr. Almeida earned his degree in Engineering from Franklin Institute in Boston, and he resides in Arlington, Massachusetts.

We welcome, you all. Every member of the panel will have 5 minutes to give their testimony, and we have a light on the table to indicate when that time is about to expire and has expired. Again, we welcome you.

And, Ms. Pallante, we will begin with you?

TESTIMONY OF THE HONORABLE MARIA PALLANTE, REGISTER OF COPYRIGHTS, U.S. LIBRARY OF CONGRESS

Ms. PALLANTE. Mr. Chairman, thank you for the opportunity to appear today, and I would also like to thank you, Ranking Member Conyers, Chairman Goodlatte, and Ranking Member Watt of the Subcommittee, and all of the Members of the Committee for your continued leadership on copyright policy.

Congress has updated the Copyright Act many times in the past 200 years, including the enforcement provisions, but as we all know, this work is never finished. Infringers today are sophisticated, and they are bold. They blatantly stream and disseminate books, music, films, and software through websites using the services of trusted search engines, advertising networks, and credit card companies. This is not a problem that we can accept. In my view, it is about the rule of law on the Internet.

Much of the bill employs a strategy of follow the money. I testified in support of this approach in March, and I still agree that it

is an important part of the equation. Many sites make money by selling illegal access to copyrighted works or by offering related advertising. But the approach does have some limitations. Many of the worst sites do not sell infringing content; they offer it for free, and they do not run ads.

I would like to offer an example involving Google, but I would first like to say that I have a great deal of respect for Google, and I cannot imagine the Internet without it. However, if you conduct a search for the phrase "download movies," Google search engine will supply the words "for free," and it will return a list of sites that offer illegal copies or streams at no charge and with no advertising. These cases require a different kind of strategy. Then, follow the money. The same is true when damages imminent, for example, when a site is streaming live sporting events or selling movies before. They have been released to the public.

In the context of foreign infringing sites, the bill addresses this problem by giving the Department of Justice, the power to require search engines to dismantle direct hyperlinks, and to require service providers to block the access of subscribers within the United States. These actions require court approval and incorporate the existing legal standards of seizure and civil forfeiture law. These are the same standards that ICE has used effectively for operation in our sites.

Mr. Chairman, I do not want to suggest that blocking websites is a small step; it is not. And the public interest groups that oppose this part of the bill are right to be concerned about unintended consequences. However, it may ultimately come down to a question of philosophy for Congress. If the Attorney General is chasing 21st century infringers, what kinds of tools does Congress want to provide? How broad and how flexible?

The bill also gives copyright owners some tools, but these do not involve search engines or ISPs, and I think that this is the right calibration. Put another way, the bill reflects the fact that many industries contribute to the success of the Internet, and it properly distinguishes between the actions that law enforcement and private citizens can bring.

One of the more interesting aspects of the bill is that before authors or other copyright owners can seek court orders, it requires them to alert payment processors and ad networks about infringing content, and request that they sever financial ties. This approach is creative and provide incentives for the parties to cooperate. It also allows for counter notification. However, whether the notification system is ultimately effective will largely depend upon whether it can be implemented in a manner that is clear and fair for all involved. The intermediaries at issue are running businesses in good faith, and the websites at issue are entitled to due process.

The bill does incorporate due process where court orders are involved. The notification system would operate outside the purview of the court, and, therefore, it may benefit from further due process review.

Finally, I do not believe it is the intent of the bill to negate the safe harbors of the DMCA, and I do not read it that way. Nothing subjects ISPs to liability for their acts or their failure to act. No monetary relief can be obtained, and the injunctive relief permitted

by the bill appears to be consistent with what the DMCA already permits. This said, the bill has many moving parts, and I note that a number of stakeholders with differing perspectives have offered productive suggestions. As the Committee works to refine the bill, I would encourage you to fully consider the suggestions. However, in closing, I would also like to state that I believe that Congress has the responsibility to protect the exclusive rights of copyright owners. And I hope that you will advance the bill with this in mind.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Pallante follows:]

Statement of
Maria A. Pallante
Register of Copyrights

Before the
Committee on the Judiciary
United States House of Represeutatives
112th Congress, 1st Session

November 16, 2011

H.R. 3261, the "Stop Online Piracy Act"

Introduction

Thank you Chairman Smith. Let me begin by expressing my appreciation to you and Ranking Member Conyers and to the many co-sponsors of the Stop Online Piracy Act (SOPA) for introducing this comprehensive proposal to combat copyright infringement on the Internet. I appreciate the opportunity to testify today.

As we all know, the Internet harbors a category of bad faith actors whose very business models consist of infringing copyright in American books, software, movies, and music with impunity. Frequently located offshore, these operators of rogue websites target American consumers and facilitate transactions using the services of search engines, advertising networks, and credit card companies. I would observe, Mr. Chairman, that this is a dark side of the Internet. In effect, we have asked American authors, publishers, and producers to invest in online commerce, but in critical circumstances we have left them to compete with thieves.

Mr. Chairman, I would like to be very clear at the outset. It is my view that if Congress does not continue to provide serious responses to online piracy, the U.S. copyright system will ultimately fail. The premise of copyright law is that the author of a creative work owns and can license to others certain exclusive rights – a premise that has served the nation well since 1790. Congress has repeatedly acted to improve enforcement provisions in copyright law over the years, including in the online environment.[1] SOPA is the next step in ensuring that our law keeps pace with infringers.

Copyright law promotes culture and free expression in the United States and is a major economic incentive. Here is how it works:

An author spends years working on a novel. As the copyright owner of that book, if she is fortunate, she may license some or all of her exclusive rights to a publisher. In editing, printing, distributing, and marketing the book, the publisher makes an investment. The publisher may offer the book to consumers through traditional bookstores or through online businesses, including those that deliver a hard copy to one's doorstep or an e-format to one's Kindle, Nook, or iPad.

Perhaps the book is timeless and universal in its appeal, making the global marketplace a possibility. The publisher may license translations of the book into multiple languages and enter into sublicenses with foreign distributors. These global distribution agreements rely upon a strong international framework for copyright protection, including reciprocal protection measures in foreign countries.

---

[1] *See* No Electronic Theft (NET) Act, Pub. L. 105-147, 111 Stat. 2678 (1997) (providing remedies for electronic infringement following reproduction or distribution in the absence of a commercial purpose or profit move); Artists' Rights and Theft Prevention Act of 2005 (ART Act), Title I of the Family Entertainment and Copyright Act of 2005, Pub. L. 109-9, 119 Stat. 218 (2005) (providing remedies for distribution on the Internet of prelease works being prepared for commercial distribution).

Let us say the novel has big screen potential. An independent producer purchases the adaptation rights, and seeks investors to make a movie possible. If the movie gets made, it will lead to additional creative authorship. For example, the producer may commission songwriters, composers, and musicians to create original musical scores and sound recordings for use in the motion picture. The film will also support multiple secondary markets, including platforms offering movies on demand, television programming, DVDs, and access through online subscriptions. There may be software adaptations, such as Wii games or other interactive products based upon the book or film, or both.

All of these licenses and business models stem from the exclusive rights that our Copyright Act provides to authors – and seeks to protect from infringers. To be clear, infringement, including at the criminal level, has been around for centuries and we will never be rid of it entirely, but this does not mean that Congress should fail to respond. Indeed, when infringers blatantly distribute, stream, and otherwise disseminate copyrighted works on the Internet, they often do so because they have no expectation of enforcement. Unfortunately, the more these kinds of actions go unchecked, the less appealing the Internet will be for creators of and investors in legitimate content. In other words, Internet piracy not only usurps the copyright value chain for any one work, it also threatens the rule of copyright law in the 21st century.

The response provided by SOPA is serious and comprehensive. It requires all key members of the online ecosystem, including service providers, search engines, payment processors, and advertising networks, to play a role in protecting copyright interests – an approach I endorse. Combating online infringement requires focus and commitment. It should be obvious that we cannot have intermediaries working at cross-purposes.

SOPA is also measured. It appropriately provides much broader tools and flexibility to the Attorney General than it provides to copyright owners. This is a sound policy choice at this time. The Department of Justice has experience fighting online infringers, will use resources carefully, must exercise prosecutorial discretion in bringing actions, and must plead its case to the court and obtain a court-issued order before proceeding. Put another way, while the copyright industries are extremely important (and certainly a point of pride with respect to the U.S. economy), SOPA recognizes that many sectors rely on, invest in, and contribute to the success of the Internet.

It is for this reason that SOPA puts only limited tools in the hands of copyright owners, and provides the Attorney General with the sole authority to seek orders against search engines and Internet service providers. This is not to say that we should not continue to assess Internet piracy and the impact of SOPA or whether additional measures or adjustments may be needed. Indeed, SOPA assigns ongoing studies to the Copyright Office and the Intellectual Property Enforcement Coordinator for these very purposes. But I do think SOPA provides the right calibration at this time.

As with any legislation, SOPA deserves and can only benefit from a robust discussion. As the Committee works to further improve and refine the bill, I know it will fully consider a variety of perspectives and suggestions, including from my fellow

witnesses. This said, I believe that Congress has a responsibility to protect the exclusive rights of copyright owners, and I urge the Committee to move forward with this in mind.

I have provided below my analysis of some of the major sections of the bill.

Attorney General: Section 102

SOPA provides 21st century tools to the Department of Justice with respect to foreign infringing websites. It allows the Attorney General to stop the participation of service providers, search engines, payment processors, and advertising networks with respect to the infringers, by obtaining court orders that are not readily available under current law. In my view, such tools are essential to stopping the economic devastation caused by rogue websites. Through SOPA, the Attorney General may also request court approval to serve orders that would require search engines to disable direct hyperlinks and service providers to block access to infringing websites, both of which could substantially reduce the number of Internet users visiting the websites, minimizing harm to the legitimate copyright owners. This does not mean that those who actively seek or wish to purchase infringing content will not be able to obtain it if they try hard enough, but SOPA would properly redirect those who erroneously believe they are purchasing copies or streams from legitimate sites.

I understand that some would prefer to limit SOPA to provisions that would allow the Attorney General to "follow the money," that is, those provisions that would starve rogue sites by severing relationships with advertising networks and payment processors. I agree that this approach is an important part of the strategy. At the same time, I note that it has some limitations in the context of the foreign infringing sites at issue in this section of the bill. Starving websites by denying them access to American commerce does not allow the Attorney General to obtain immediate relief, even when the evidence is overwhelming and the damage is imminent – such as situations involving live sporting events or sales of pre-release films. Nor will it be effective against willful infringers who cause immense damage by allowing users to download and stream copyrighted works for free.

My own view is that there will be times when blocking access to websites may be the only quick and effective course of action and that providing this tool to the Attorney General is therefore a critical part of the equation. Likewise, I believe that search engines should be fully within the reach of the Attorney General and should be ordered in appropriate circumstances to dismantle direct hyperlinks that send unwitting consumers to rogue websites. As I explained in my previous testimony, this does not mean that blocking should be conducted in a manner that would jeopardize the operation of the Internet.[2] However, in working to perfect these particular aspects of SOPA, I would encourage Congress to continue to consult experts who can objectively evaluate any

[2] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I Before the Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. (2011) (statement of Maria A. Pallante, Acting Register of Copyrights), *available at* http://judiciary.house.gov/hearings/pdf/Pallante03142011.pdf.

technical concerns and who appreciate the goal of providing law enforcement with sufficiently flexible tools.

By way of illustration, these kinds of "irreversible" infringements have been the focus of the "Operation In Our Sites" initiative by which U.S. Immigration and Customs Enforcement (ICE) has seized domestically registered domain names using existing seizure and civil forfeiture laws, thereby rendering the infringing sites temporarily dysfunctional. Since launching the operation in June 2010, ICE has seized 200 domain names and redirected users to a banner[3] stating that the domain names were seized and that willful copyright infringement and intentionally and knowingly trafficking in counterfeit goods are criminal offenses. Eighty-six of the 200 domain names have been forfeited to the U.S. government thus far.[4]

Seizure and civil forfeiture laws have been effective for criminal infringements because they allow ICE to pursue the source of infringing activity. Specifically, 18 U.S.C. § 981 allows the Attorney General to seize certain property subject to forfeiture in the United States. Section 2323 of Title 18 allows forfeiture of, among other things, articles prohibited by 17 U.S.C. § 506 (criminal copyright infringement), 18 U.S.C. § 2319 (criminal copyright infringement for violations of 17 U.S.C. § 506(a)), 18 U.S.C. § 2319A (unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances), and 18 U.S.C. § 2319(B) (unauthorized recording of motion pictures in a motion picture exhibition facility). Section 2323 also authorizes forfeiture of property used to commit or facilitate such infringements.

SOPA incorporates these standards by reference: the definition of a "foreign infringing site" for purposes of the Attorney General action includes the requirement that the site would "be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site." The legislation essentially protects American consumers from the actions of bad actors who have a direct impact on American copyright businesses and consumers, but who are located outside the borders of the United States.

Some have stressed, and I agree, that due process is important in the context of legislating a solution to rogue websites. Due process is a bedrock foundation of our nation's legal system, even for those who violate the law. Any remedy that impedes or obstructs access to a website must be consistent with this core American principle. The affected parties should receive notice as well as an opportunity to be heard.

SOPA includes general principles of due process by incorporating Federal Rule of Civil Procedure 65. Rule 65 provides that an adverse party is entitled to notice and an opportunity to be heard before issuance of a temporary restraining order unless "(A) specific facts in an affidavit or a verified complaint clearly show that immediate and

---

[3] *See* ICE announces results of 'Operation Strike Out' - Protects consumers from counterfeit sports paraphernalia on the Internet and on the streets, Oct. 31, 2011, *available at* http://www.ice.gov/news/releases/1110/111031washingtondc.htm.

[4] *Id.*

irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." Thus, the rule limits *ex parte* orders to extraordinary circumstances.

Stopping infringement at the borders is not a new concept of American copyright law. Customs and Border Protection (CBP) has long had the authority to prevent infringing physical goods from entering U.S. commerce, even without advance notice or a hearing under certain circumstances.[5] International standards are also instructive. The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement provides that governments should have the ability to seize infringing hard goods at the border based on evidence provided by the right holder.[6] An importer must receive notice of the seizure (or suspension as it is referred to in international law), but not before the suspension takes place.[7]

It also bears repeating that injunctions are not at odds with the First Amendment. As noted First Amendment scholar Floyd Abrams has observed, they are "a longstanding, constitutionally sanctioned way to remedy and prevent copyright violations."[8] In fact, "*no* court has ever denied [ ] [that] injunctions are a valuable and constitutional response to copyright violations."[9] At the same time, Mr. Abrams has noted that a "zero tolerance" policy – "where an entire website could be blocked or seized for a single, or just a few, offenses – would plainly raise the most troublesome First Amendment concerns."[10] I share the same concerns about a "zero tolerance" approach, but that is not SOPA.

Marketplace Notification and Injunctive Relief: Section 103

Section 103 of SOPA would allow copyright owners who have suffered harm to seek relief against foreign and domestic infringing websites, serving as a complement to the authority of the Attorney General. Unlike the Attorney General, however, copyright owners would not be able to block domain names or websites or otherwise affect the underpinnings of the Internet. Nor does SOPA permit monetary relief for copyright owners. By targeting sites dedicated to infringement and permitting injunctive relief only, it limits the incentive for copyright owners to overreach.

---

[5] *See* 19 U.S.C. § 1595A; 19 C.F.R. §§ 133.42, 133.43.

[6] *See* TRIPS Art. 51.

[7] *See id.* Art. 54.

[8] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II Before the Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. (2011) (statement of Floyd Abrams).

[9] *Id.* (emphasis in original); *see also N. Y. Times v. United States*, 403 U.S. 713, 731 n. 1 (1971) (White, J. concurring) ("no one denies that a newspaper can properly be enjoined from publishing the copyrighted works of another.").

[10] Floyd Abrams Statement, *supra* n. 8.

Under this section, SOPA defines an infringing website as one: (1) that "is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in, offering goods or services in a manner that engages in, enables, or facilitates" a violation of 17 U.S.C. §§ 501, 1201 or certain trademark law provisions; (2) where the operator "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the [site] to carry out acts that constitute [infringement];" or (3) where the site is operated "with the object of promoting, or has promoted, its use to carry out [infringement] as shown by clear expression or other affirmative steps to foster infringement."

I would like to underscore that subsection 103(a)(1)(B)(ii)(I) in the definition described above sets forth a willful blindness standard. This is important because it would encompass situations where an infringer takes deliberate action to avoid knowledge of the infringement, in cases where there is a high probability of infringement.[11] At the same time, it provides a blueprint for companies that build their businesses in good faith, by confirming that those who respect copyrighted content will not be put at a competitive disadvantage for doing so.

As a procedural matter, SOPA permits copyright owners to bring *in personam* actions against the registrant of a domain name or the operator of a rogue website, or, in certain circumstances, an *in rem* action against that website or the domain name used by such site, and to serve copies of those orders on payment processors and advertising networks. They may only do so, however, if they first send notices to the payment processors and advertising networks pursuant to the notification system SOPA creates. The notices must identify the infringing Internet site and describe the specific facts supporting the claim that the site is infringing as well as the irreparable injury, loss, or damage that would result if timely action were not taken. A site owner or operator can immediately challenge this notification by serving a counter notification stating that the site is not in fact an infringing site. Upon receipt of an effective counter notification, an advertising network or payment processor need not take any further action unless and until it has been served with a court order.[12]

SOPA's notification process is innovative in spirit. It empowers copyright owners, but potentially limits the need for litigation by providing a mechanism for them to work directly with payment processors and advertising networks. It also provides incentives for the latter to cooperate voluntarily when notified that they are dealing with a site dedicated to infringement, rather than being compelled to do so by court order.

---

[11] *See Global-Tech Appliances v. SEB S.A.*, 131 S.Ct. 2060 (2011) (setting forth willful blindness standard as meeting the knowledge requirement for inducing infringement of a patent case, a doctrine closely related to inducing infringement of a copyright).

[12] SOPA requires advertising networks or payment processors to take action within five days of receiving an initial notice, but it does not require them to wait the full five days and thus there is no set time frame during which a payment processor or advertising network must wait to see if a counter notification is filed.

Whether the notification process will ultimately be effective may in large part depend on the volume of notices received and whether payment processors and advertising networks will feel compelled to process and respond to them in the absence of a court order. If it appears likely that some may respond while others may not, I would encourage Congress to consider further refinements. Congress will want to ensure that those who are less conscientious do not emerge with a marketplace advantage over those who choose to work with copyright owners in good faith, and it will want to ensure that the businesses of the websites are not unduly affected. The goal is to achieve the participation of payment processers and advertising networks in shutting down infringers while also ensuring general due process protections for all involved.

As introduced, SOPA provides a good start in this regard. For example, the copyright owner must include a statement that the notification is made in good faith, is accurate, and the signatory to the notification is authorized to act on behalf of the holder of the intellectual property right. Indeed, copyright owners are often in a good position to ascertain useful and reasonably detailed information about infringing websites and it is my view that they should share as much information as reasonably possible with the intermediaries whose help is sought. SOPA also provides significant penalties for misrepresentations contained in a notification, including damages, costs, and attorneys fees. As stated above, SOPA also provides for a counter notification, and at this stage of the process does not create consequences if the intermediary fails to act.

Once the copyright owner commences an action with the court, Rule 65 of the Federal Rules of Civil Procedure applies. As noted above, that Rule generally requires notice and an opportunity to be heard, unless the movant satisfies the stringent requirements for an *ex parte* order. In addition, the plaintiff cannot serve copies of the orders on payment processors or advertising networks without court approval. Again the consequences are limited, even at this stage of the process. If the intermediary fails to sever ties with the website, there is no infringement liability, only an order from the court to comply and possible penalties if they refuse and are held in contempt.

Nor, contrary to the assertions of some critics of SOPA, does this notification affect the safe harbors that Internet service providers enjoy under the Digital Millennium Copyright Act (DMCA). Section 512 of Title 17 provides safe harbors from liability for damages and limits the scope of injunctive relief for service providers who comply with its requirements. Nothing in SOPA subjects service providers to liability for their acts or their failures to act. No monetary relief may be obtained against a service provider pursuant to SOPA, apart perhaps for sanctions for contempt of court if a service provider does not comply with a court order. The injunctive relief permitted by SOPA is within the scope of the limitations in section 512(j), which provides, in the case of "transitory digital network communications," that a service provider may be restrained "from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States" (compare to Section 102(c)(2)(A)(i) of SOPA), and that an Internet search engine may be subject to such injunctive "relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location,

if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose." (Compare to Section 102(c)(2)(B) of SOPA.)

Streaming

Mr. Chairman, I would also like to say how pleased I am that SOPA would harmonize the options available to prosecutors in cases of willful, criminal infringement, as between the exclusive rights of reproduction, distribution, and public performance. As I have previously testified, the right of public performance is of growing importance in the marketplace, because the streaming of copyrighted works is an increasingly important means by which copyright owners provide access.

Unfortunately, prosecutors are placed at a disadvantage and have a disincentive to pursue cases of willful, criminal streaming because (unlike instances of willful reproduction or distribution) the maximum possible penalty is a misdemeanor. This lack of parity neither reflects nor serves the marketplace. Video streaming traffic is among the fastest growing areas of the Internet and now accounts for more than one quarter of all Internet traffic. Consumers now have numerous ways to enjoy streamed content legally through legitimate video streaming websites like Hulu or Netflix, user generated content sites like YouTube, and streaming music services. Streamed content, including sports programming, is also often provided legally by content owners through their own websites and Internet portals such as ABC.com and HBO GO. And today users can even stream content through applications on their smart phones or their video game consoles. Indeed, in a very real sense, the innovative technology companies that contract with creators in good faith and pay licensing fees as a cost of doing business are as victimized by piracy as those who create the content in the first instance.

I am particularly pleased that SOPA would update the provisions that govern pre-release scenarios (scenarios where infringers offer a television program, sporting event, movie, or other copyrighted work prior to the date of public release, causing especially egregious harm). SOPA recognizes that streaming is a major means of pre-release infringement and provides prosecutors with a clear basis to take action.

While it should be clear from my statements here that the streaming provisions of SOPA are based on longstanding legal principles, I would like to address some of the concerns and misunderstandings these proposals have generated. First, not all streaming is at issue. The provisions at issue are criminal provisions. They are not applicable to innocent activity or activity that might legitimately be categorized as fair use. Criminal copyright infringement requires a finding that the offender acted "willfully," which courts generally interpret as meaning a "voluntary intentional violation of a known legal duty."[13] SOPA does not alter that standard. Similarly, it would not negate the innocent infringement doctrine in civil actions nor subject a party to any liability that it does not already have with respect to reproducing or distributing a copyrighted work. I believe

[13] *See* 4 Melville B. Nimmer and David Nimmer, Nimmer on Copyright 4 § 15.01[A][2] (Matthew Bender, Rev. Ed.) ("|T|he better view construes the 'willfulness' required for criminal copyright infringement as a 'voluntary, intentional violation of a known legal duty.'").

this is clear in SOPA, but if necessary, the distinction between criminal and innocent infringement could be clarified.

Copyright Office

Finally, I note that SOPA would bestow a number of important responsibilities on the Copyright Office, including a study of the legislation once implemented and an ongoing obligation to work with the Secretary of State and Secretary of Commerce to ensure that the protection in foreign countries of U.S. persons' intellectual property rights is a significant component of U.S. foreign and commercial policy. We will of course be very pleased to undertake these responsibilities and more, so that creators and intermediaries alike can flourish in the online environment.

Thank you Mr. Chairman.

Mr. SMITH. Thank you, Ms. Pallante.
Mr. Clark?

TESTIMONY OF JOHN P. CLARK, CHIEF SECURITY OFFICER AND VICE PRESIDENT OF GLOBAL SECURITY, PFIZER, INC.

Mr. CLARK. Chairman Smith, Ranking Member Conyers, distinguished Members of the Committee——

Mr. WATT. Could you pull your mic a little bit closer, please, or cut it on?

Mr. CLARK. It is a pleasure to appear before you today to discuss the threat that counterfeit medicines posed to the health and safety of patients in the United States and around the world. It is a closer global issue.

As Vice President of Global Security for Pfizer, I work to mitigate the threat that counterfeit medicines posed to the health and safety of patients who rely on Pfizer medicines to live healthier and longer lives. I commend the Chairman and the Ranking Member of on the Committee for co-sponsoring the Stop Online Piracy Act for their legislative effort. It is a positive step forward in our fight against counterfeit medicines.

Counterfeit medicines pose a threat because of the conditions under which they are manufactured, on unlicensed, unregulated sites, frequently under unsanitary conditions. In many instances, they contain none of the active pharmaceutical ingredients found in authentic medicines or in incorrect dosages, depriving patients, depriving patients of the therapeutic benefit of the medicine prescribed by their put physicians. And others, they may contain toxic ingredients, such as heavy metals, arsenic, pesticides, rat poison, brick dust, floor wax, leaded highway paint, and even sheet rock or wallboard.

Counterfeit medicines are a global problem, and I am pleased to share our experience in combating them, and how the Stop Online Piracy Act aims to strengthen the U.S. arsenal.

Pfizer has implemented an aggressive anti-counterfeiting campaign that attacks counterfeits at their source. Since 2004, we have prevented more than 138 million dosages of counterfeit Pfizer medicines alone, more than 68 million finished dosages, and enough active pharmaceutical ingredients to manufacture another 70 million from reaching global patients. Additional raid by law enforcement, based on evidence we have provided have also resulted in seizures of millions of dosages of counterfeits marketed by other major pharmaceutical companies.

In the United States, we work closely with ICE, the FBI, and FDA on their investigations, and with Customs and Border Protection to improve their ability to prevent counterfeit Pfizer medicines from reaching U.S. patients. While the true scope of the counterfeit problems is hard to estimate, we have confirmed that counterfeit Pfizer medicines have been found and seized and at least 101 countries, and have reached the supply chains and 53 countries.

Technology has created a new front in this battle. Today the major threat to patients in the U.S. are the many professional looking websites that promise safe, FDA approved, branded medicines from Canada or the UK, and for that reason, we appreciate the Chairman and Ranking Member's focus on the threat in Title I of

the bill, giving the Attorney General new tools and incentivizing private stakeholders to act against rogue websites, with immunity in place for every stakeholders' action would be an important step forward.

Patients do not realize that many of the websites do not disclose the true source of the products they dispense, or even where their alleged dispensing online pharmacy is located. In such instances, the World Health Organization has estimated that patients have more than a 50 percent chance of receiving a counterfeit medicine. I happen to believe that is a very low estimate.

I would like to share two short case studies. The first is Rx North. Patients who visited Rx North's website thought they were ordering from a Canadian pharmacy and would receive authentic FDA approved medicines. In reality, the medicines dispensed from our Rx North were traced from China, where they were manufactured, through Hong Kong, on to Dubai, into the UK where they were intercepted. Among the medicines seized by UK customs were Lipitor, found to contain only 82 to 86 percent of the active pharmaceutical ingredient, which is an incredibly high number for most counterfeit, as well as counterfeit versions of medicines from four other companies, including one found to contain traces of metal.

The second is the case of Kevin Xu, convicted of misbranding drugs and trafficking in counterfeit goods. It demonstrates how attractive a target the U.S. supply chain is who account for those who counterfeit our medicines, and how weak our current penalties for counterfeiting medicine are.

During meetings with our undercover consultant, Xu boasted of the global scope of his criminal enterprise. He offered a list of branded counterfeit medicines that he could provide, including five Pfizer medicines. The evidence we gathered was shared with an ongoing ICE investigation of Xu. An order placed by an ICE undercover agent was filled with the counterfeit. When the tablets were tested, they were found to contain only insignificant levels of the active pharmaceutical ingredient found in the authentic medicine.

Xu was sentenced to just 78 months in Federal prison without parole, the maximum sentence under the applicable U.S. sentencing commission guideline range. This punishment does not reflect the seriousness of the crime. The Stop Online Piracy Act takes a positive step toward making these penalties even tougher.

Pharmaceutical counterfeiting is a low risk, high profit criminal activity that has attracted drug traffickers, fire arms smugglers, and terrorists. One of the principal players in the 2003 Lipitor breach here in the U.S. was a convicted cocaine trafficker. In 2006, the U.S. attorney for the Eastern District of Michigan announced the indictment of 19 people who gave a portion of their profits from the sale of counterfeit Viagra to Hezbollah.

Those who counterfeit medicines are confident that even if caught, they will get just a slap on the wrist. Even here in the U.S., the maximum sentence imposed under the Food and Drug and Cosmetics Act is just 3 years. Recognizing the inherent risk that any counterfeit medicine poses to patients, we must enhance the penalties for pharmaceutical counterfeiting to provide a greater deterrent. Expedited procedures must be in place to shut down rogue websites dispensing counterfeit medicines to the U.S.

The Stop Online Piracy Act is a significant step forward in those efforts, and I thank the Chairman and Ranking Member for introducing this important piece of legislation. I would like to work with you so that our laws recognize the grave health and safety risk posed by counterfeit medicines and serve as a deterrent.

I work with foreign government representatives in the global fight against counterfeiting. It is hypocritical for us to speak with foreign government representatives, as I often do, about their lack of effective legislation, when U.S. laws are still lacking. This bill, if enacted, with strong penalties and mechanism to shut down rogue websites will be highly effective in our global argument for all governments to fully appreciate the serious health and safety aspects of this problem, and encourage similar efforts around the world.

Thank you again for this opportunity to express my views. For Pfizer, pharmaceutical counterfeiting is first and foremost an issue of patient health and safety. We look forward to working with you on the global fight against counterfeit medicines.

[The prepared statement of Mr. Clark follows:]

Prepared Statement of John P. Clark, Chief Security Officer, Pfizer, Inc. and Vice President, Global Security

Chairman Smith, Ranking Member Conyers, distinguished Members of the Committee. It is indeed a pleasure to appear before you today to discuss an issue of great importance—the threat that counterfeit medicines pose to the health and safety of patients in the United States and around the world.

My name is John Clark, and I am the Chief Security Officer for Pfizer Inc, and Vice President of its Global Security Team. In those positions I am responsible for ensuring that programs are in place to protect Pfizer's personnel, real and intellectual property, reputation, and the integrity of its medicines.

Prior to joining Pfizer in 2008, I served as Immigration and Customs Enforcement (ICE) Deputy Assistant Secretary, responsible for the overall management and coordination of the agency's operation, as well as the Assistant Secretary's principal representative to the Department of Homeland Security and to the law enforcement and intelligence communities. During my more than 25 years in ICE and its predecessor agency, U.S. Customs, I held a variety of investigative, management and executive positions.

Pfizer is a diversified, global health care company and the world's largest biopharmaceutical company. Our core business is the discovery, development, and marketing of innovative pharmaceuticals for human and animal health, and we are committed to ensuring the integrity of those products when they reach the market.

THREAT TO PATIENT HEALTH AND SAFETY

A significant aspect of my job is to mitigate the threat that counterfeit medicines pose to the health and safety of patients who rely on Pfizer medicines to live healthier, longer lives. For that reason, I commend the Chairman and Ranking Member and the many members who are co-sponsors of the Stop Online Piracy Act for their legislative effort. It is a positive step forward in our fight against counterfeit medicines.

Counterfeit medicines pose a threat because of the conditions under which they are manufactured—in unlicensed and unregulated sites, frequently under unsanitary conditions—and the lack of regulation of their contents. In many instances, they contain none of the active pharmaceutical ingredient (API) found in the authentic medicine, or an incorrect dosage, depriving patients of the therapeutic benefit of the medicines prescribed by their physicians. In others, they may contain toxic ingredients such as heavy metals, arsenic, pesticides, rat poison, brick dust, floor wax, leaded highway paint and even sheetrock or wallboard.

Counterfeit medicines are a global problem, one from which no region, country, therapeutic area is immune. And, while my comments today focus on Pfizer's experience in combating counterfeit medicines and the positive impact the Stop Online Pi-

racy Act can make in that effort, it is a threat to the entire pharmaceutical industry.

PFIZER'S PROGRAM TO MITIGATE THAT THREAT

We have implemented an aggressive anti-counterfeiting campaign to detect and disrupt major manufacturers and distributors of counterfeit Pfizer medicines. By attacking counterfeits at or near their source, we protect the global market. Through our efforts we have, since 2004, prevented more than 138 million doses of counterfeit Pfizer medicines—more than 68 million finished doses and enough active pharmaceutical ingredient to manufacture another 70 million—from reaching patients around the world. And, because those who counterfeit our medicines have no "brand loyalty", raids by law enforcement authorities based on evidence we have provided have also resulted in seizures of millions of doses of counterfeits marketed by other major pharmaceutical companies.

I attribute the success of our program to our talent—colleagues placed strategically around the world with extensive law enforcement experience who know how to initiate and develop cases—and the effective partnerships we have forged with enforcement authorities around the world. As part of those partnerships, we not only refer the results of our investigations, but also provide support as required in investigations and test—free of charge—suspected counterfeit Pfizer medicines to determine their authenticity.

We also provide training to enforcement authorities to raise awareness to the counterfeiting problem and enhance their ability to distinguish counterfeit from authentic Pfizer medicines. As of September 30, 2011, we have provided training to authorities in 117 countries, often in conjunction with programs sponsored by the US Patent and Trade Office (USPTO) and the World Customs Organization (WCO). In some instances, we have sponsored regional conferences to facilitate collaboration between authorities in the regions, and work with them to develop actionable plans of action to address the problem.

These training efforts have produced tangible results in increased enforcement activity in Egypt, Jordan, Lebanon, the UAE and Poland, and the passage of strong anti-counterfeiting legislation in Jordan and Kenya.

In the U.S., we work closely with ICE, the FBI and FDA on their investigations, and with CBP to improve their ability to prevent counterfeit Pfizer medicines from reaching U.S. patients.

One example of our collaboration with CBP is the use of our "mobile labs", which we have used in pilot programs with CBP at International Mail Facilities in San Francisco, Los Angeles, New York, Miami and Chicago.

While the true scope of the counterfeit problem is hard to estimate, we can provide some metrics based on the seizures reported to us by enforcement authorities and confirmed by our labs. Based on that data, we have confirmed counterfeit Pfizer medicines in at least 101 countries, and having breached the legitimate supply chains of 53.

While Viagra is our most counterfeited medicine, counterfeiters have targeted more than 50 of our products, including Aricept (*Alzheimers),* Celebrex (*anti-inflammatory*), Genotropin *(human growth hormone*), Lipitor *(high cholesterol*), Metakelfin *(anti-malarial*), Norvasc *(high blood pressure*), Prevnar *(vaccine to prevent infection caused by pneumococcal bacteria*), Sutent *(for treatment of treatment of rare cancer of the stomach, bowel or esophagus (GIST), advanced kidney cancer (RCC, and a type of pancreatic cancer (pNET),* Viagra *(erectile dysfunction*), Xanax *(anxiety disorders*), Zithromax *(anti-infective)* and Zoloft (*depression*).

And counterfeit versions of 23 of those medicines, including Celebrex, Genotropin, Lipitor, Metakelfin, Norvasc, Prevnar, Sutent, Viagra, Xanax and Zithromax, have breached supply chains around the world.

THE ONLINE THREAT

The major threat to patients in the U.S., however, is the Internet and the many professional looking websites that promise safe, FDA-approved, branded medicines from countries such as Canada or the UK. And, for that reason, we appreciate the Chairman and Ranking Member's focus on that threat in Title I of the bill. Giving the Attorney General new tools and incentivizing private stakeholders to act against rogue websites if immunity is in place for every stakeholder's actions would be an important step forward.

Patients are lured by the ease with which they can order their medicines online, often without the need to consult a doctor or provide a valid prescription. They do not realize that many of those sites have failed to disclose the true source of the products they dispense or even where they—the "dispensing" online pharmacy are located. In such instances, the WHO has estimated that patients have more than a 50% chance of receiving a counterfeit medicine.

It is possible for U.S. patients to buy their medicines safely online through pharmacies that have been accredited by the National Association of Boards of Pharmacies (NABP). To be accredited, a pharmacy must comply with the licensing and inspection requirements of their state and each state to which they dispense pharmaceuticals. If they meet these criteria they are designated VIPPS sites—Verified Internet Pharmacy Practice Sites. Pharmacies displaying the VIPPS seal have demonstrated to NABP compliance with VIPPS criteria including patient rights to privacy, authentication and security of prescription orders, adherence to a recognized quality assurance policy, and provision of meaningful consultation between patients and pharmacists. VIPPS pharmacies represent only a small percentage of online pharmacies. In a recent survey of more than 8000 websites selling medicines, the NABP found that 96% were not operating in accordance with pharmacy laws and standards.

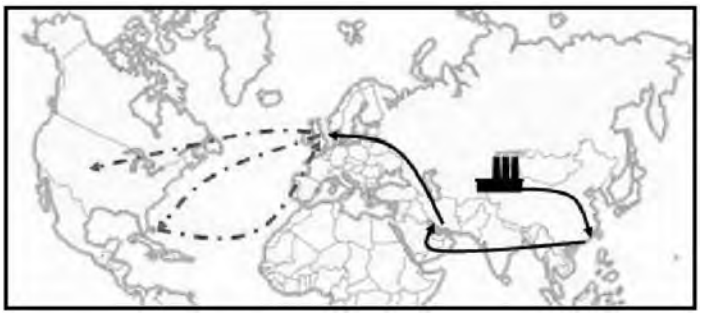
CASE STUDY: RXNORTH

The case of RxNorth is an excellent example of how easily patients can be deceived, and the risks to which they expose themselves when ordering online from a rogue website, which the Stop Online Piracy Act aims to shutdown.

Patients, who visited the RxNorth website, thought they were ordering from a Canadian Pharmacy and would receive authentic FDA-approved medicines.

In reality, however, the medicines dispensed from RxNorth were traced from China, where they were manufactured, through Hong Kong, Dubai, to the UK where they were intercepted. Among the medicines seized by UK Customs were Lipitor—found to contain only 82 to 86% of the claimed dosage of active pharmaceutical ingredient—as well as counterfeit versions of medicines from four other companies, including one found to contain traces of metal.

Subsequent investigation revealed that had they not been intercepted, those medicines would have been sent to a fulfillment center in the Bahamas, where they would have been split from their pallets and placed in individual packages corresponding to customer order. To gain "credibility", the packages would then have been shipped to the UK, from where they would have been sent to the U.S. patients who had placed their orders with RxNorth, believing it to be a "safe" pharmacy in Canada.



As a result of this investigation, the FDA warned consumers not to place orders with RxNorth and not to take the medicines they had received. But, more needs to be done to combat these rogue websites.

CASE STUDY: OPERATION CROSS OCEAN

Operation Cross Ocean also demonstrates the threat to unsuspecting U.S. patients who order their medicines online. Chinese and U.S. authorities worked together to dismantle an operation that manufactured counterfeit versions of Viagra and other medicines in China, then dispensed them via the Internet through a network of brokers, largely in the U.S. and Europe.

When they raided the manufacturing site (pictured below), authorities seized 10 lines of manufacturing equipment and counterfeit medicines, including 570,000 finished pills and enough active pharmaceutical ingredient to manufacture 1.82 million more.

CASE STUDY: KEVIN XU

The case of Kevin Xu, convicted of misbranding drugs and trafficking in counterfeit goods, demonstrates how attractive a target the U.S. supply is for those who counterfeit our medicines and how weak our current penalties for counterfeiting medicines are.

An investigation initiated in our Asia-Pacific region identified Xu and his company, Orient Pacific International, as a major manufacturer and distributor of counterfeit medicines, including several Pfizer products. During meetings with our "undercover" consultant, Xu boasted of the global scope of his criminal enterprise, including his responsibility to oversee the quality of counterfeits produced in China, and provided a list of branded medicines that he could provide, which included Pfizer's Alzheimer's drug, Aricept, ulcer drug, Cytotec, cholesterol lowering drug, Lipitor, kidney cancer drug, Sutent and erectile dysfunction drug, Viagra.

The evidence we gathered was shared with ICE, which had already begun an investigation of Xu. An order placed by an ICE undercover was filled with counterfeit Aricept, Pfizer's Alzheimer's drug, packaged for the French market. When the tablets were tested, they were found to contain only insignificant levels of the active pharmaceutical ingredient found in authentic Aricept.

Xu was arrested in July 2007 and charged with manufacturing counterfeit versions of medicines intended to treat prostate cancer (Casodex, Astra Zeneca), blood clots (Plavix, Bristol Myers Squibb), schizophrenia (Zyprexa, Lilly), and Alzheimers (Aricept, Pfizer), mislabeling them as chemicals, and smuggling them into the U.S. where they were to be introduced into our supply chain.

The likelihood of Xu's success was high. European authorities have identified Xu as the source of counterfeit versions of non-Pfizer products—Zyprexa (Lilly, anti-psychotic), Plavix (Bristol Myers Squibb, blood thinner), and Casodex (Astra Zeneca, prostate cancer) –recalled from the legitimate supply chain in the UK, a supply chain as tightly regulated as ours, in May 2007.

As reported in a press release by the U.S. Attorney's Office for the Southern District of Texas, Xu was "sentenced to 78 months in federal prison without parole, the maximum sentence under the applicable U.S. Sentencing Commission guideline range for conspiring with others in the Peoples Republic of China to traffic in counterfeit pharmaceutical drugs and causing the introduction of counterfeit and misbranded drugs into interstate commerce." *http://www.cybercrime.gov/XuSent.pdf*, accessed on November 10, 2011

This is a good example of the punishment not rising to the level of the seriousness of the crime and why we need stronger penalties. The Stop Online Piracy Act takes a positive step forward and we would welcome the opportunity to work with you to perfect the penalty section.

CASE STUDY: ARAB CHINA NETWORK

Based upon information provided by Global Security, more than 300 Chinese law enforcement officers, from both the Public Service Bureau (PSB) and State Food and Drug Administration (SFDA), initiated enforcement actions that dismantled one of the most prolific counterfeiting organizations ever uncovered in China. The network, comprised of males of Middle East descent living in the southern provinces of China, was responsible for distributing large quantities of counterfeit medicines, manufactured in China, throughout the Gulf States and U.S..

In two separate but related enforcement operations, authorities raided two manufacturing sites and 26 storage facilities, making 26 arrests. They seized vast amounts of finished products—a mix of counterfeits and generics—including counterfeit Pfizer's ulcer drug, Cytotec, Viagra and Pfizer's anti-anxiety drug, Xanax. Initial estimates by authorities placed the pill count as high as 200 million, including counterfeits of Pfizer medicines as well as those of four other pharma companies. Also seized were large quantities of active pharmaceutical ingredient, including barrels of sildenafil, the active pharmaceutical ingredient in Viagra, which may be beyond the capability of the authorities to accurately weigh. The seizures included equipment—54 machines and 1230 moulds, tools and dies, at least 200 of which are for Pfizer medicines—with which to manufacture the counterfeits.

In a subsequent release to Chinese Media, authorities stated that they had seized approximately 7 million counterfeit Viagra in those raids.

CASE STUDY: OPERATION EAGLE EYE

Based on information provided by Pfizer, China's Ministry of Public Security (MPS) raided sites in Eagle Eye Action in Henan, Zhezjang, Guangdong provinces, making 36 arrests. They seized more than 5.6 million counterfeit tablets including medicines from Pfizer (Aricept, Lincocin, Lipitor, Viagra, Xanax) and two other major pharmaceutical companies, as well as 45 machines.

The head of the operation was sentenced to life imprisonment. Other members of the criminal network received sentences ranging from 2 to 15 years in jail.

WHAT MORE CAN WE DO?

We have seen progress in the fight against counterfeit medicines, but much more needs to be done. In some countries, pharmaceutical counterfeiting is not a crime; in others it has only minimal sanctions. Lax enforcement of laws that do exist is yet another problem.

Pharmaceutical counterfeiting is a low risk, high profit criminal activity that has attracted drug traffickers, firearm smugglers, and, even terrorists. One of the principal players in the 2003 Lipitor breach here in the U.S. was a convicted cocaine trafficker. In 2006, the U.S. Attorney for the Eastern District of Michigan announced the indictment of 19 people who gave a portion of their profits from the sale of counterfeit Viagra to Hezbollah.

Those who counterfeit medicines are confident that even if they get caught, they will get a mere slap on the wrist. Even here in the U.S., the maximum sentence imposed under the Food Drug and Cosmetics Act is 3 years. Recognizing the inherent risk that any counterfeit medicine poses to patients, we must enhance the penalties for pharmaceutical counterfeiting to provide a greater deterrent. Expedited procedures must be put in place to shutdown "rogue" websites dispensing counterfeit medicines to U.S. patients.

The Stop Online Piracy Act is a significant step forward in those efforts and I thank the Chairman and Ranking Member for introducing this important piece of legislation. I would like to work with you so that our laws recognize the grave health and safety risks posed by counterfeit medicines and serve as a deterrent.

I work with foreign government representatives in the global fight against counterfeiting. It is hypocritical for us to speak with foreign government representatives, as I do, about their lack of effective legislation when U.S. law is still lacking. This bill, if enacted with strong penalties and mechanisms to shut down rogue websites, will be highly effective in our global argument for all governments to fully appreciate the serious health and safety aspects of this problem and encourage similar efforts.

CONCLUSION

Thank you again for this opportunity to express my views. For Pfizer, pharmaceutical counterfeiting is first and foremost an issue of patient health and safety. We look forward to working with you on the global fight against counterfeit medicines.

Mr. SMITH. Thank you, Mr. Clark.
Mr. O'Leary?

TESTIMONY OF MICHAEL P. O'LEARY, SENIOR EXECUTIVE VICE PRESIDENT, GLOBAL POLICY AND EXTERNAL AFFAIRS, MOTION PICTURE ASSOCIATION OF AMERICA (MPAA)

Mr. O'LEARY. Thank you. Mr. Chairman, Ranking Member Conyers, Chairman Goodlatte, and Ranking Member Watt, distinguished Members of the Committee, I am honored to be here today and, and thank you for holding this important hearing. I also want to thank you for introducing this legislation, which will help protect American creativity and American jobs from thieves who hide overseas and seek to profit off the hard work of people in this country.

I also want to acknowledge my fellow panelists. I am pleased to be here with all of them today, and look forward to working with them throughout this process. I want to particularly acknowledge the contributions of Ms. Kirkpatrick and MasterCard. As the Chairman alluded to earlier, they are truly a fine example of a corporation trying to make the Internet a safe marketplace for people all over the world. And frankly, their example is one to be followed.

Critics would have you, as Mr. Watt alluded to, believe that this is a battle between two giant corporations, and there is certainly a lot of truth to that. But I am also very proud to be part of a wide ranging coalition that includes the AFL-CIO, who we will hear from shortly, members of the Chamber of Commerce, big business, small business, individual creators, and entrepreneurs. So, I think critics would have you believe that this bill is really about supporting Hollywood and things like that, but the truth of the matter, when you look behind the rhetoric and the hyperbole, is that intellectual property is something which affects every facet of the American economy, and it affects people all over the country.

In the case of the industry that I represent, the American motion picture and television industry, we believe that these jobs are worth protecting. They are more fully detailed in my written testimony, but I would just mention a few. There are people like Dan Lemieux, who is a stunt coordinator from Michigan. He has worked on numerous films and television shows like Nip Tuck and The

Shield. The industry includes over 95,000 small businesses. They employ 10 people or less. Businesses like Fletcher Camera, which is in Chicago. They have 25 employees in that small business, and they provide movie equipment for productions that occur all over the Midwest. There are hundreds of thousands of businesses that provide services to production. There is a small paint and decorating firm in Baltimore, Maryland. It is a fifth generation family run operation, and it has applied paint for virtually every major production, which has occurred in the mid-Atlantic region over the past few years.

I want to be very clear with this Committee that hard work, innovation, and creativity are not solely the province of people who live in northern California. There are people all over this country who contribute to the economy every day, who contribute to our culture, who contribute to what we make creatively. And their jobs are just as important and just as worth protecting as anyone else's. And that is why we think this bill is so important, because it is a positive step in that direction.

In this economic climate, we simply cannot afford to turn our back on any industry, which is coming forward and producing things that we can take all over the world and be successful with. Our industry competes. When we are given an opportunity to compete globally, we succeed. Where we have trouble, frankly, Mr. Chairman, is where we do not have an opportunity to compete fairly. And one of the problems we have is competing with people who are trying to steal our stuff. We are not before the Congress looking for a handout or a bail out. We are simply asking for an opportunity to stop from stealing the products that we make.

In recent weeks, you have heard a lot of spurious arguments about this legislation. They have been chronicled in a number of the opening remarks, that it violates the First Amendment, that it undermines existing protection laws, that it somehow stifles innovation, and that it will, yes, break the Internet. The irony, of course, of that argument is that I believe it was first raised by those opposing the DMCA many years ago, as the Chairman will recall. And I believe some of those same people are here today opposing this bill because they think it will undermine the DMCA. So, there is a bit of irony there, which seems to be lost inside the Beltway, but I suspect that, outside the Beltway people see it for what it is.

These allegations that you are hearing are simply taken from the playbook of those people who have consistently opposed every effort that the Congress has come forward with in the past few years to protect intellectual property. The good news is that every time Congress protects intellectual property, the Internet flourishes. Every time the United States stands for legitimacy over illegitimacy, the Internet gets bigger and stronger. More things are available to consumers. More products are available to consumers. We make more movies. They see more television. Protecting legitimacy is a positive thing for the economy and for innovation, and people that tell you otherwise are wrong. They have been wrong when they have been raising these arguments for the past two decades, and they are wrong in the context of this bill.

What you understand so clearly, Mr. Chairman, and the Stop Online Piracy Act reflects this, is that there is a very great difference between legitimate marketplace and the illicit sites and services that we are talking about. When the legitimate market is protected against the threat of online theft, the only people who lose are those who do not work, take no risk, make no investment. Instead, those are the people that simply try to profit off the hard work of others.

We have also heard arguments that Congress should limit its approach to the threat of rogue sites to "following the money." It is worth noting that whoever usually makes that argument is really saying you should follow someone else's money. If we are, in fact, going to follow the money, which is something we should do, we should follow all of the money, not just some of it.

Piracy is a complex problem that cannot be fixed in piecemeal solutions, but this bill is an important first step in trying to deal with what is a very real and growing threat. This is fundamentally about jobs and about protecting the jobs that Americans have, creating products that are enjoyed all over the world.

Ultimately, someone once said that to lead is to choose, and the bill, Mr. Chairman, that you put before the Congress in this debate is one which provides a number of choices. It is a choice between illegal and legitimate. It is a choice between a safe, vibrant Internet for everyone and all black-market Internet. It is a choice between protecting American creativity and jobs or protecting thieves. These are simple choices from our perspective, and with the leadership that has been provided by this Committee, we look forward to this process, debating this bill, putting something on the President's desk that both Republicans and Democrats can support, and at the end of the day, will allow these hard-working Americans to keep their jobs and keep creating the products that the world enjoys. Thank you.

[The prepared statement of Mr. O'Leary follows:]

STATEMENT OF MICHAEL P. O'LEARY,
SENIOR EXECUTIVE VICE PRESIDENT,
GLOBAL POLICY AND EXTERNAL AFFAIRS,
ON BEHALF OF
THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

BEFORE THE HOUSE JUDICIARY COMMITTEE

HEARING REGARDING
H.R. 3261, THE "STOP ONLINE PIRACY ACT"

RAYBURN HOUSE OFFICE BUILDING, ROOM 2141
WASHINGTON, D.C.

WEDNESDAY, NOVEMBER 16, 2011
10 A.M.

The Film and Television Industry and Its Contribution to the U.S. Economy

Chairman Smith, Ranking Member Conyers, and members of the Committee, thank you for holding this hearing regarding H.R. 3261, the Stop Online Piracy Act, an important new bill to protect jobs and the economy by taking action against foreign rogue websites and illegal cyberlockers that traffic in stolen creative works.

I appreciate the opportunity to testify on behalf of the Motion Picture Association of America, Inc.[1] and its member companies regarding the impact of this illicit activity on our business and the livelihoods of those who work in our industry, and how H.R. 3261 will help address this challenge.

[1] The Motion Picture Association of America and its international counterpart, the Motion Picture Association (MPA), serve as the voice and advocate of the American motion picture, home video and television industries, domestically through the MPAA and internationally through the MPA. MPAA members are Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc.

Fundamentally, this is about jobs. The motion picture and television industry supports more than two million American jobs in all 50 states. The 20 states and Puerto Rico represented by this Committee are home to 1.7 million American jobs supported by the motion picture and television industry, including more than 525,000 direct motion picture and television industry jobs. About 12 percent of those are directly employed in motion picture and television production and distribution, jobs paying an average annual salary of nearly $79,000. Those are not just the people whose names you see on the marquee in front of the theater – they're the hard-working people behind the scenes, from the carpenter who built the set, to the costumer and make-up artist who helped bring each character to life, to the Foley artist who created the sound effects. They are people like Dan Lemieux, a stunt coordinator in Michigan, who depends on the residual payments he earns to help support his wife and three children between productions. Dan was the stunt coordinator for the "Ides of March" and has done stunts for television programs like "Charmed", "Nip/Tuck" and "the Shield.

Our industry also includes more than 95,000 small businesses across the country that are involved in the production and distribution of movies and television, the vast majority of which employ fewer than 10 people. These are businesses like Fletcher Camera & Lenses in Chicago, whose full-time staff of 25 employees works to provide equipment for film, television, and commercial productions in the Midwest.

And beyond even these are the hundreds of thousands of other businesses that every year provide services to productions, like the local drycleaner that served the cast and crew on location or the local hardware store that supplied paint and lumber. For example, Budecke's Paints & Decorating of Baltimore, Maryland, a fifth-generation family-owned and-operated retailer, which has supplied paint for virtually every major production filmed in the area in recent years. The motion picture and television industry made $38.9 billion in payments to more than 208,000 such businesses in 2009. On average, a major motion picture shooting on location contributes $225,000 every day to the local economy.

Every day, these people go to work to create a product – one of our country's most creative, most innovative, most widely-recognized and most beloved products. And every day, over and over, that product is stolen, sometimes with nothing more than the click of a mouse. To these men, women, and their families, online content theft means declining incomes, reduced health and retirement benefits, and lost jobs. This rampant theft cannot continue, and the Stop Online Piracy Act will help accomplish that goal.

Websites Trafficking in Stolen Digital Content Create Consumer Confusion, Harm the Legitimate Marketplace and Damage Our Industry

Let me make one thing very clear at the outset. In recent weeks, Mr. Chairman, you and your colleagues have heard a great deal from those who suggest this bill, and our efforts to fight online theft, will "break the Internet" or harm legitimate online social media platforms and Internet services. Nothing could be farther from the truth.

When someone turns on a cell phone or a computer or a gaming system, often their purpose is to watch a movie or a TV show. The Internet and related digital distribution systems are a critically important avenue for growth for our industry, and every day, we are pursuing even more new and innovative ways to deliver our content to our consumers. Compromising those opportunities would hurt us, our partners, and our customers. What you have understood so clearly, Mr. Chairman, and what the Stop Online Piracy Act reflects, is the very great difference between that legitimate marketplace and the illicit sites and services that are dedicated to the theft of copyrighted works.

Currently, the most pernicious forms of digital theft occur through the use of so-called "rogue" websites or cyberlockers. These platforms – I will refer to them today as "rogue sites" for simplicity – facilitate the illegal distribution of copyrighted works through many different forms, including streaming, downloading, or linking to another site or service offering unauthorized content.

These rogue sites, whose content is hosted and whose operators hide around the world, are increasingly sophisticated in appearance and take on many attributes of legitimate content delivery sites, creating additional enforcement challenges and feeding consumer confusion. Many rogue sites accept credit cards or "e-wallet" alternatives to facilitate payments, display advertising for mainstream, blue-chip U.S. companies, and offer rewards programs for frequent purchasers. In addition, these often legitimate-looking websites expose consumers to criminals, who routinely collect personal and financial information from unsuspecting targets, subjecting those consumers not only to fraud and deceit, but also to identity theft and other harms.

The proliferation of these rogue sites undercuts the legitimate market for filmed entertainment and thus the financial support for future film and television

production, threatening earnings and jobs throughout the U.S. Even major motion pictures newly in theaters appear on these rogue sites just days, if not hours, after their theatrical release – exploited for profits by thieves who did not work, took no risk, and invested no resources in the production of those films.

Furthermore, legitimate companies that want to invest in and develop new and innovative business models centered around high-quality online content and greater consumer choice have a limited potential for growth when they are forced to compete with entities that are distributing the exact same content through illicit means. That is not innovation – it is theft.

Some who oppose this bill claim that the Digital Millennium Copyright Act (DMCA) is sufficient to combat online theft. As you know, Mr. Chairman, the DMCA created a model whereby rights holders may notify a website containing infringing content and ask that it be removed. And where these sites are legitimate and make good faith efforts to respond to our requests this model works with varying degrees of effectiveness. It does not, however, always work quickly, and it is not perfect, but it works.

But the rogue websites and cyberlockers I have just described are not legitimate. They do not act in good faith. They do not comply with DMCA requests, because their purpose is to traffic in stolen content. And when they are based overseas, they can simply thumb their noses at U.S. law.

Criminals are not standing still, and if our efforts to protect American creativity are to succeed, the law cannot stand still either. That is why we need this bill.

The Stop Online Piracy Act is a Smart, Reasonable Approach to Combat the Threat of Rogue Sites

The Stop Online Piracy Act recognizes that to effectively stop online theft, ***every*** member of the Internet ecosystem needs to play a role, including the rights holders who created the content, the Internet Service Providers and search engines that connect consumers to rogue sites, and the advertising networks and payment processors that provide those sites with financial support. There are three specific elements of this bill Mr. Chairman, that I want to address this morning.

Narrowly Defined to Target Only Rogue Sites
First, it is clear from the language of H.R. 3261 that it is meant to apply only to rogue websites, and not to legitimate platforms. The definitions in the bill are very narrow and rooted in longstanding Supreme Court precedent with which U.S. based sites must already comply. For the bill to apply, a site must be "otherwise subject to seizure if it were a U.S. site" or primarily designed or operated for the purpose of copyright infringement, or deliberately turning a blind eye to violations of U.S. law, or taking "affirmative steps" to "foster infringement" such as rewards programs and prizes for uploading stolen content. These narrow definitions would not apply to legitimate businesses, like Twitter or Facebook. Legitimate sites are not covered by this legislation.

Provides Rogue Sites with Robust Due Process
Second, the Stop Online Piracy Act provides very strong due process protections to alleged rogue sites – in fact, ***it provides foreign-based sites*** with exactly the same procedural protections afforded U.S. citizens under the Federal Rules of Civil Procedure. This includes requiring prosecutors to notify the site and its registrants or owners of their intent to act under the bill, and to notify any intermediary that may be ordered by the court to discontinue providing services to that site. As such, domain name owners or site operators would have every right to defend themselves in court should they choose to do so.

Equally strict standards would apply in cases where a content owner seeks to act to prevent online theft by a rogue site. Contrary to wild assertions bandied about by those who oppose this legislation, H.R. 3261 does not give content owners the power to shut down websites. The bill sets out a new voluntary notification process that encourages private, out-of-court solutions as the preferred means to efficiently and effectively protect against the enormous losses that result from content theft. Indeed, the bill contains provisions that will provide immunity for voluntary action against sites dedicated to the theft of U.S. property or sites that endanger public health.

At the same time, the bill preserves the ability of rights holders to seek limited injunctive relief in the courts against a rogue website if intermediaries choose not to take action against a website. Rights holders must clearly show, as they would under Federal Rule of Civil Procedure 65, that immediate and irreparable injury, loss, or damage will result in the absence of timely action. Content owners that file frivolous or unsupported claims could face damages, including costs and attorneys' fees.

Takes a Comprehensive Approach that Closes a Loophole in Current Law
Third and finally, the Stop Online Piracy Act also includes other enhancements to current copyright law to prevent online content theft. One of these applies to the treatment of infringing content that is delivered using streaming technology. While existing law makes an infringement of any of the copyright owner's exclusive rights a criminal act when done willfully and for commercial advantage or private financial gain, felony penalties only apply to defendants engaged in the illegal *reproduction* or *distribution* of copies of one or more copyrighted works meeting specified numerical and monetary value thresholds.

As technology has advanced since enactment of these provisions, however, so too have the means of willful and commercially destructive infringement. Increasingly, copyrighted content is not only made available for unauthorized downloading, but now is frequently streamed illegally as well. But our laws have not caught up with the thieves, and as a result, uncertainty remains whether unauthorized Internet streaming of copyrighted works can be prosecuted as a felony, as other forms of piracy are. H.R. 3261 closes that loophole in our nation's intellectual property laws. In so doing, it eliminates an unjustified, technology-specific disparity between forms of infringement that have increasingly similar commercially-destructive impacts.

To be clear: making available and profiting from an illegal, unauthorized stream of copyrighted content is already a crime. Content thieves should not be able to escape tougher penalties simply by choosing a different technology to perpetrate their crime.

Critics' Arguments Ignore History of Copyright Legislation, Misread H.R. 3261

In recent weeks, as you know Mr. Chairman, there has been no shortage of critics attacking this legislation. Often, unfortunately, these are many of the same voices that claim to support the protection of intellectual property yet seem reflexively to oppose every effort to actually enact effective protections. I'd like to conclude my testimony by addressing the three main arguments on which these objections rest.

H.R. 3261 Will Not "Break the Internet"
Critics claim that requiring Internet intermediaries to take steps that would prevent links to rogue sites from functioning would "break the Internet" and jeopardize the

online security protocol known as Secure DNS, or DNSSEC. We see three problems with this claim.

First, technology like site blocking and filtering, is employed around the world today to deal with spam, malware, viruses and all manner of bad behavior, including for copyright protection with no adverse impact on the Internet. There is no reason to suggest that the use of this technology by intermediaries in the U.S. would lead to a different result.

Second, some have suggested the Internet would "break" because, they claim, huge numbers of U.S. consumers will rush to employ non-U.S. Internet services in order to access infringing content, driving traffic offshore and undermining Internet security. Yet, this is all based on one erroneous assumption: that all consumers who may now find themselves using rogue sites will keep doing so even in the face of a court order deeming those sites to be illegal. Consumers do not look for rogue sites when they search, they look for content – and the Stop Online Piracy Act will help ensure that the content they find is legitimate. The only people encouraging the use of an alternate domain system are thieves seeking to keep their lucrative black market alive and avoid detection.

Third, opponents point to the DNSSEC code and claim that it is not compatible with the site blocking or filtering technology envisioned by H.R. 3261. This argument conveniently ignores not only the history of the creation of DNSSEC but also the very nature of Internet protocols, which is simply this: when new developments or circumstances require changes to these codes, *the codes change*. Any software engineer will tell you that no development process stops at version 1.0. Today is no different. As Daniel Castro of the Information Technology and Innovation Foundation wrote earlier this year, the issue with DNSSEC "appears to be the result of a deficiency in the current DNS protocol (perhaps a result of the ideological stance of its authors) rather than any true technical limitation. [2]

H.R. 3261 Does Not Undermine Free Expression – It Protects It

Critics also claim that the Stop Online Piracy Act would violate the First Amendment or threaten the freedom of expression. This, too, is inaccurate. The motion picture and television industry depends on the First Amendment to protect our ability to freely create the very content that rogue sites are stealing. As noted First Amendment scholar Floyd Abrams wrote just last week regarding H.R. 3261: "Copyright violations have never been protected by the First Amendment and have

[2] Daniel Castro, "No, COICA Will Not Break the Internet, Innovation Policy Blog, 1/18/11

been routinely punished wherever they occur, including the Internet. This proposed legislation is not inconsistent with the First Amendment; it would protect creators of speech, as Congress has done since this Nation was founded, by combating its theft." The Stop Online Piracy Act imposes no prior restraint on speech and its underlying principle is well established in U.S. law.

Further, it is absurd to suggest that passing legislation to take action against rogue sites would provide shelter to repressive regimes that wish to censor political speech. There is a key distinction between protecting property versus restricting speech. That distinction is enshrined in the U.S. Constitution and in the International Declaration of Human Rights. Indeed, the enactment of the Stop Online Piracy Act would instead be a strong signal to other nations of America's commitment to protecting speech and preventing theft.

H.R. 3261 Will in No Way "Stifle Innovation" and Investment in Technology
Lastly, opponents of this legislation threaten that passing H.R. 3261 will lead to the curtailment of investment in new technology ventures and will even "stifle innovation" online. We have heard this argument before. Many of the loudest voices opposing rogue sites legislation are the same critics who predicted disaster in the wake of the DMCA, the Net Act and the unanimous Supreme Court decision in Grokster. Yet, since those events occurred, the Internet has grown by leaps and bounds, innovation is off the charts and access to technology is at an all time high.

Take a look at venture capital. In 2005, the National Venture Capital Association warned that a Supreme Court ruling holding Grokster liable would "have a chilling effect on innovation." They could not have been more wrong. Since that decision, venture capital investment in media and entertainment has been one of the fastest growing sectors of the venture capital market. Contrary to naysayers' claims, strong copyright law promotes innovation. The MPAA studios are engaged in multiple new on-line businesses, there are more than 350 legal online services around the world that provide high-quality video on demand, including more than 60 services in the United States. Disney announced Disney Studio All Access in February which provides consumers with easier access to Disney content, Time Warner announced a partnership with Facebook in March to distribute film and television shows through Warner Brothers Entertainment's Facebook fan page, and the list goes on. Additionally, many of these services are free unlike rogue websites. Those who say otherwise have been wrong again and again, and are wrong today.

* * *

Mr. Chairman, Ranking Member Conyers, again I thank you and this Committee on behalf of our member companies for the opportunity to testify today.

As you know very well, this legislation is ultimately not about technology. This is, fundamentally, about the foundation on which American industry has rested for over two hundred years: the expectation that someone who creates a great product, a product consumers want, will be able to reap the rewards of his or her creative work.

Intellectual property theft – online or on the street – subverts that promise. In doing so, it steals from people who deserve better: in the case of film and television, from over two million Americans, some of the hardest-working, most imaginative, most creative and innovative people in our country, who invest their time, energy and resources to create extraordinary filmed entertainment enjoyed by millions around the world.

We cannot simply stand by and let this theft go unchecked. For that reason, we urge the speedy approval of the Stop Online Piracy Act, and we pledge to do all we can to support your efforts to bring rogue sites legislation to the President's desk.

Again, thank you for holding this important hearing and I'd be happy to answer any questions you may have.

Mr. SMITH. Thank you, Mr. O'Leary.
Ms. Kirkpatrick?

TESTIMONY OF LINDA KIRKPATRICK, GROUP HEAD, CUSTOMER PERFORMANCE INTEGRITY, MASTERCARD WORLDWIDE

Ms. KIRKPATRICK. Thank you. Good morning, Chairman Smith, Ranking Member Conyers, and Members of the Committee. My name is Linda Kirkpatrick, and I am group head, franchise development and customer performance and integrity at MasterCard Worldwide in Purchase, New York.

MasterCard commends the Committee on its attention to the issue of Internet-based infringement, including the work that went into H.R. 3261, the "Stop Online Piracy Act." We greatly appreciate the opportunity to be here today, and look forward to working with you to combat this critical issue.

MasterCard's rules and requirements prohibit the use of its system for any illegal purposes, including for the sale of products or services that infringe on intellectual property rights. MasterCard recognizes the important role it plays in combatting this issue, and has taken a number of steps that demonstrate its commitment to this important cause.

These efforts, which are discussed in my written testimony, include: publishing the MasterCard anti-piracy policy, which sets out the specific process by which MasterCard and rightsholders can work together to identify and prevent the sale of infringing products or services; working with the White House's Office of U.S. Intellectual Property Enforcement coordinator in the development of industry best practices to address online infringement; and the implementation and maintenance of MasterCard's business risk assessment and mitigation program, otherwise known as our BRAMA program.

By way of background, MasterCard operates a global payment system that connects over 1 billion cardholders and millions of merchants worldwide to complete MasterCard branded payment transactions. MasterCard neither issues payment cards to cardholders, nor does it contract with merchants to accept payment cards. Rather, MasterCard's financial institution customers issue payment cards to cardholders, and contract with birches to accept the cards.

The card issuing customers are known as issuers; those customers that contract with merchants for card accepted are commonly called acquirers. Each cardholder's account relationship is with the issuer that issued the card to the cardholder, and each merchant's acceptance relationship is with its acquirer.

MasterCard has a long history of working with law enforcement, private stakeholders, its customers, and others, to address illegal or otherwise BRAM damaging activities that may involve the MasterCard payment system or the unauthorized use of our widely recognized family of payment brands. Our commitment to working with rightsholders to prevent the MasterCard system from being used to facilitate online infringement is evidenced by our industry leading anti-piracy policy, which is publicly available on our Internet site.

In accordance with that policy, MasterCard has established procedures that apply when a law enforcement entity or rightsholder brings to MasterCard's attention evidence of alleged infringement. We have established an e-mail address for the submission of such

requests and a set of information requirements for such requests, which are largely similar to the information required of rightsholders in H.R. 3261.

The process we implemented was developed collaboratively through strong working relationships with rightsholders and their trade associations, and has led to the investigation of thousands of Internet sites, and the termination of hundreds of rogue merchants.

MasterCard has also worked closely with the White House's Office of U.S. Intellectual Property Enforcement coordinator in the development of a best practices document to address online infringement. Development of the best practices document involved input from a wide variety of stakeholders, including numerous representatives from the rightsholder community, payment networks, and other parties involved in online commerce. The best practices are designed to assist rightsholders in protecting their intellectual property through a voluntary system, and in no way diminish the ability of rightsholders to take independent action to enforce their intellectual property rights.

Our business risk assessment and mitigation program, or BRAM program, is another key component of MasterCard's corporate effort to preserve the integrity of the MasterCard payment systems and protect against illegal and BRAM damaging transactions. More specifically, the Bram program serves to restrict access to the MasterCard system by merchants whose products and services may pose significant fraud, regulatory, or legal risks.

The BRAM program was created to enforce MasterCard rules, prohibiting acquirers from engaging in or supporting any merchant activity that is illegal, or that may damage the good will of MasterCard, or reflect negatively on the MasterCard brand. Merchant activities that infringe upon the intellectual property rights of another are expressly covered under the protocols of the BRAM program.

MasterCard is fully committed to continuing to address this important issue. As the Committee moves forward with legislation, MasterCard believes it is essential to ensure that any obligations imposed on payment systems are capable of being readily implemented through reasonable policies and procedures, and that payment systems be shielded from litigation and liability when acting in accordance with the bill's requirements. Thank you. In my written testimony, we have offered a few general comments on the bill along those lines that we believe are consistent with the Committee's objectives.

I look forward to answering any questions that you may have.

[The prepared statement of Ms. Kirkpatrick follows:]

HEARING ON H.R. 3261, THE "STOP ONLINE PIRACY ACT"

TESTIMONY OF LINDA KIRKPATRICK
GROUP HEAD, FRANCHISE DEVELOPMENT / CUSTOMER PERFORMANCE INTEGRITY
MASTERCARD WORLDWIDE

BEFORE THE COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

NOVEMBER 16, 2011

Good morning, Chairman Smith, Ranking Member Conyers, and Members of the Committee. My name is Linda Kirkpatrick, and I am Group Head, Franchise Development/Customer Performance Integrity, at MasterCard Worldwide ("MasterCard") in Purchase, New York. It is my pleasure to appear before you today to discuss the important issue of combating the sale of infringing goods over the Internet. We commend the Committee on its attention to this issue, including the hard work that has gone into drafting H.R. 3261, the Stop Online Piracy Act. We greatly appreciate the opportunity to be here today and we look forward to working with you to combat this critical issue going forward.

MasterCard's rules and requirements prohibit the use of its system for any illegal purposes, including for the sale of products or services that infringe on intellectual property rights, and we are vigilant in our efforts to prohibit the sale of infringing products or services and other illegal or reputation-damaging products or services through the MasterCard system. MasterCard recognizes the important role it plays in combating this issue and has taken a number of steps that demonstrate its commitment to this important cause. These efforts, which are discussed in greater detail below, include: (i) publishing the MasterCard Anti-Piracy Policy, which sets out the specific process by which MasterCard and rights holders can work together to identify and prevent the sale of infringing products or services; (ii) working with the White House's Office of the U.S. Intellectual Property Enforcement Coordinator in the development of

industry best practices to address copyright infringement and the sale of counterfeit products over the Internet; (iii) the implementation and maintenance of MasterCard's Business Risk Assessment and Mitigation ("BRAM") Program to protect MasterCard against efforts to use the MasterCard system for illegal or brand-damaging activities; and (iv) the development of programs to combat the illicit online sale of pharmaceuticals and the use of the Internet for the sale of child pornography.

Background on MasterCard

MasterCard advances global commerce by providing a critical link among more than 21,000 financial institutions and millions of businesses, cardholders and merchants worldwide who use MasterCard's global payment system to complete MasterCard-branded payment card transactions. MasterCard licenses its customers around the world to use the MasterCard service marks in connection with those payment card transactions. Importantly, MasterCard neither issues payment cards to cardholders, nor does it contract with merchants to accept payment cards. Rather, MasterCard's financial institution customers issue payment cards to cardholders and/or contract with merchants to accept the cards. The card-issuing customers are known as "issuers." Those customers that contract with merchants for card acceptance are commonly called "acquirers." Each cardholder's account relationship is with the issuer that issued the card to the cardholder, and each merchant's acceptance relationship is with its acquirer.

Typical Transaction

When a MasterCard-branded credit card is used to make a purchase at a brick-and-mortar merchant, the card typically is swiped through a terminal which reads basic information about the card (*e.g.*, card number and expiration date) from the magnetic stripe on the back of the card.

For Internet-based transactions, this information typically is captured by the merchant by prompting the cardholder to enter the basic information in an electronic form. This information is linked together with the dollar amount and date of the transaction, as well as basic information about the merchant. A message containing the information is then transmitted to the acquirer that signed up the merchant to accept the card. This is known as the "authorization message."

The acquirer routes the authorization message to MasterCard and MasterCard then routes the authorization message to the issuer. The issuer checks to make sure that there is sufficient credit associated with the cardholder's account to cover the transaction and that the card has not been reported as lost or stolen, and then sends to MasterCard a message authorizing the transaction. MasterCard then routes the message to the acquirer, which transmits the message back to the merchant to authorize the transaction. In the MasterCard system, an authorization request and response is completed, on average, in 120 milliseconds. A second message, called the "clearing message," generally is sent later in the day to confirm that the transaction has been completed and to initiate the movement of funds. The clearing message follows the same route from the acquirer to MasterCard, and then back to the issuer. The issuer uses that record to post the transaction to the cardholder's account. Once clearing is completed, a daily reconciliation is provided to each customer to facilitate the exchange of funds between issuers and acquirers. The process of moving funds from issuers to acquirers is known as the "settlement" process.

MasterCard's Efforts to Prevent Infringing Online Sales and Other Illicit Online Activities

In General

At MasterCard, we take our responsibility as a corporate citizen very seriously. MasterCard has a long history of working with law enforcement, private stakeholders, its

customers, and others to address illegal or otherwise brand-damaging activities that may involve the MasterCard payment system or the unauthorized use of our widely recognized family of payment brands.

A fundamental rule of our system is that each customer must conduct its MasterCard programs and activities in accordance with all applicable laws. This includes, for example, the obligation of an acquirer to ensure that any transaction the acquirer submits into the MasterCard system pertains only to legal activity. MasterCard also has a series of rules that require acquirers to ensure that the merchants with whom they contract to accept MasterCard-branded cards are legitimate and engage only in legal activities. These rules mandate, among other things, that an acquirer perform due diligence on a merchant before enabling the merchant to accept MasterCard-branded cards. These rules also require acquirers to monitor merchants for compliance with these rules. Customers that fail to comply with these rules may be required to absorb the cost of any illegal transactions, and may be subject to assessments, suspension or termination. MasterCard has forged strong working relationships with rights holders and their trade associations. This collaboration has led to the investigation of thousands of Internet sites and the termination of hundreds of rogue merchants.

MasterCard also works extensively with law enforcement officials to address situations where the legality of activities related to MasterCard-branded payment card transactions is in question. For example, in the U.S., MasterCard works with a variety of federal and state law enforcement agencies on these issues generally, including state Attorneys General, the Drug Enforcement Administration, the Food and Drug Administration, the U.S. Secret Service, the Federal Bureau of Investigation, and other branches of the Department of Justice. A major objective of these efforts is to ensure that MasterCard provides appropriate support to law

enforcement in their efforts to address illegal activity. We recognize that our efforts to enforce the MasterCard rules have the potential to unintentionally hinder ongoing law enforcement investigations. For example, when an acquirer shuts off MasterCard acceptance with a merchant because the merchant violated MasterCard's rules, law enforcement's ability to gather evidence through MasterCard's system can be impeded. Further, the merchant may suspect that it is the subject of an ongoing investigation. Accordingly, we work closely with law enforcement and will act in accordance with instructions from law enforcement officials, including by not taking action that could compromise an investigation.

MasterCard's Anti-Piracy Policy

MasterCard's commitment to preventing the use of MasterCard-branded payment cards in connection with the online purchase of goods or services that violate intellectual property rights is evidenced by our industry leading Anti-Piracy Policy, which is publicly available at http://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf and a copy of which is attached as APPENDIX A. In accordance with that policy, MasterCard has established procedures that apply when a law enforcement entity or rights holder brings to MasterCard's attention the online sale of a product or service that allegedly infringes copyright or trademark rights of a party.

These procedures are complex, as they involve multiple constituents in the payments value chain, each of which has a role to play in an investigation. When a law enforcement entity is involved in the investigation and provides MasterCard with evidence of illegal activity, MasterCard will first endeavor to identify the acquirer that has the relationship with the alleged infringing merchant. MasterCard performs a test to determine whether the Internet site in

question actually accepts MasterCard-branded payments and, if so, to identify the acquirer for the Internet site. The timing for completion of this process depends in part on the speed at which a merchant submits payment transactions into the system. Many times after conducting a test of payment acceptance, we determine that an Internet site that purports to accept MasterCard-branded payments, in fact, does not. If MasterCard believes that its brand is being used in connection with alleged illegal activity, it will require the relevant acquirer to conduct its own investigation and, within two business days, provide a written report to MasterCard setting forth the results of the investigation and any steps taken to address those results.

If the acquirer determines that the merchant was engaging in the sale of an infringing product or service, the acquirer must take the actions necessary to ensure that the merchant has ceased accepting MasterCard-branded cards as payment for an infringing product or service. If the acquirer determines that the merchant was not engaging in the sale of an infringing product or service, the acquirer must provide to MasterCard compelling evidence of this conclusion. If the acquirer decides to terminate the merchant, MasterCard will require that the acquirer add the merchant to a MasterCard database for terminated merchants, if applicable, and thereby afford other acquirers notice that the merchant has been terminated and of the reason code used by the acquirer for the termination.

When a law enforcement entity is not involved, a rights holder may notify MasterCard of its belief that the online sale of a product or service violates its intellectual property rights and request that MasterCard take action on such belief. MasterCard generally will also accept such notices from a rights holder's trade association. Significant collaboration with the rights holder community has led to the development of this notification process, and MasterCard is committed to maintaining an open dialogue with rights holders.

To facilitate a notification from a rights holder, MasterCard has established an email address for the submission of such requests and a set of information requirements for such requests. The information requests must include a description of the alleged infringement, evidence that a MasterCard-branded payment card can be used to purchase the allegedly infringing product, a copy of the rights holder's cease and desist letter or Digital Millennium Copyright Act notice or an appropriate attestation from the rights holder, and evidence that the rights holder owns the intellectual property in question.

Upon receipt of a notice that meets the information requirements, MasterCard will endeavor to identify the acquirer that has the relationship with the merchant. As noted above, the timeframe within which the acquirer is identified varies based on factors that may be beyond MasterCard's control. MasterCard will require an identified acquirer to investigate the alleged illegal activity and, within five business days, provide a written report to MasterCard setting forth the results of the investigation and any steps taken to address those results. The measures required of an acquirer upon a determination that the merchant is, or is not, engaged in the sale of an infringing product or service are the same for both rights holder and law enforcement notifications to MasterCard. Because rights holder notices do not carry the certainty that comes with a law enforcement notice, these investigations often require more time to complete. In some cases, it may be necessary to afford an acquirer additional time to complete its investigation and other obligations before an accurate assessment of the merchant's activities can be made. Following receipt of the results of an acquirer's investigation, MasterCard will inform the rights holder (or trade association) of those results.

Collaboration with the U.S. Intellectual Property Enforcement Coordinator

In addition to the development and implementation of the MasterCard Anti-Piracy Policy, MasterCard worked closely with the White House's Office of the U.S. Intellectual Property Enforcement Coordinator in the development of a "best practices" document to address copyright infringement and the sale of counterfeit products over the Internet. Development of the best practices document involved input from a wide variety of stakeholders, including numerous representatives from the rights holder community, payment networks, and other parties involved in online commerce. The best practices document prescribes clear and transparent procedures for payment networks to address sales of infringing products and counterfeit trademark products over the Internet. The best practices are designed to assist rights holders in protecting their intellectual property through a voluntary system and in no way diminish the ability of rights holders to take independent action to enforce their intellectual property rights. The MasterCard Anti-Piracy Policy incorporates the best practices and, indeed, exceeds the standards established in the best practices document.

MasterCard Efforts to Address Other Illegal or Brand-Damaging Internet-based Activities

BRAM Program. MasterCard is dedicated to preserving the strength and value of the MasterCard family of brands and strives to ensure that the MasterCard marks are not in any way associated with illegal or brand-damaging activities. The BRAM Program is a key component of these corporate efforts and is designed to preserve the integrity of the MasterCard payment system and protect against illegal and brand-damaging transactions. More specifically, the BRAM Program serves to restrict access to the MasterCard system by merchants whose products and services may pose significant fraud, regulatory, or legal risks. The BRAM Program was

created to enforce MasterCard rules prohibiting acquirers from engaging in or supporting any merchant activity that is illegal or that may damage the goodwill of MasterCard or reflect negatively on the MasterCard brand. Merchant activities that infringe upon the intellectual property rights of another are expressly covered under the protocols of the BRAM Program.

Other activities addressed by the BRAM Program include the sale or offer of sale of a product or service other than those in full compliance with applicable law, and the sale of a product or service, including an image, which is patently offensive and lacks serious artistic value. As part of the BRAM Program, MasterCard uses a sophisticated Internet monitoring service designed to ensure that MasterCard has robust and current profiles of high-risk merchants doing business in the MasterCard system. This enables MasterCard to monitor its system for illegal and brand-damaging merchant activities and proactively pursue remedial actions with acquirers that may unknowingly be facilitating transactions for merchants engaged in infringing or other illicit activities.

Combating Child Pornography. MasterCard has partnered with the National Center for Missing and Exploited Children ("NCMEC") in the U.S., and its international counterpart, the International Centre for Missing & Exploited Children, to form the Financial Coalition Against Child Pornography ("Coalition"). The Coalition represents a partnership of companies and governmental entities that have come together to combat perpetrators of child pornography, including criminals who traffic in child pornography on the Internet. It includes a broad range of financial institutions, Internet service providers, and technology companies committed to working with NCMEC and governmental agencies to develop a coordinated approach to detecting and combating child pornography and to provide a critical mechanism for assisting law

enforcement in developing the information needed to apprehend and prosecute persons who perpetrate child pornography crimes.

Illicit Internet Sales of Pharmaceuticals. MasterCard has partnered with a number of private-sector companies involved in the online payments, advertisement, and shipping industries to establish the Center for Safe Internet Pharmacies ("CSIP") in an effort to prevent illicit Internet sales of pharmaceuticals. The chief goals of the CSIP are to educate consumers about the dangers of the illegal sale of prescription pharmaceuticals and to provide a forum for working with law enforcement to take legal action against merchants involved in this process. The CSIP also provides a forum for the sharing of information by and among private-sector entities and global governmental agencies regarding the illicit online advertisement and distribution of prescription pharmaceuticals.

H.R. 3261, the Stop Online Piracy Act

MasterCard supports the Committee's efforts to address the issue of Internet sales of infringing products or services. As noted above, MasterCard is fully committed to continuing to do our part to address this important issue. As the Committee moves forward with legislation to address the sale of infringing products or services over the Internet, MasterCard believes it is essential to ensure that any obligations imposed on payment systems are capable of being readily implemented through reasonable policies and procedures, and that payment systems be shielded from litigation and liability when acting in accordance with the bill's requirements. Accordingly, we wish to identify a number of key areas where we believe that changes to the bill would ensure that MasterCard can continue to play an appropriate and effective role. We are committed to working with the Committee as the bill moves forward to help improve the bill in a

manner that is consistent with its objectives, and we appreciate the opportunity to offer specific comments and suggestions on the bill to the Committee.

Five-Day Timeframe. The bill provides that payment network providers must take certain measures within five days after being served with a copy of an order or receiving a notice from a rights holder. Upon receiving a copy of an order or receiving notice from a rights holder, there are many circumstances that may arise which make a five-day window to complete the required actions not workable for a four-party payment network, such as MasterCard. For example, simply identifying the acquirer for an Internet site may take several days depending upon how long it takes for the alleged infringer to submit payments to its acquirer. The process becomes even more complex if the acquirer does not respond or asks for an extension because of local jurisdiction or other issues. Additionally, providing the merchant an opportunity to respond (in the case of a notice from a rights holder) also requires time. Moreover, confirming that a merchant may no longer accept payment from our brand for an infringing product may also take time. MasterCard is committed to begin this process within five days. However, MasterCard urges the Committee not to set an artificial deadline for the performance of a specific action as it may present impossible compliance challenges in some circumstances.

Certification Requirement. Under the bill, service of a copy of a court order by a rights holder on a payment network provider would trigger an obligation of the payment network provider to file with the court a certification of receipt not later than seven days after service. In MasterCard's view, this obligation would impose material costs on payment network providers without a commensurate benefit. The process would require additional employee resourcing, the retention of qualified local counsel, and the payment of any applicable court fees. Moreover, the bill provides a rights holder the ability to seek the imposition of monetary sanctions on a

payment network provider that does not comply with the court certification process, even though rights holders also have a remedy if a payment network provider does not take the required measures in response to a court order. The certification and sanctions approach is at odds with the cooperative approach that MasterCard and others have taken in their efforts to work together against online intellectual property piracy through the best practices and, in the case of MasterCard, our Anti-Piracy Policy.

Liability. We are grateful to the Committee for incorporating into the bill several essential protections against liability for payment network providers. However, it is important that the bill be clarified regarding the liability protection for payment network providers that receive notice from a rights holder of an allegedly infringing Internet site. While the bill contemplates that a rights holder may pursue a court order against such a site if a payment network provider does not complete certain required actions within the five-day window of time, the bill does not provide that the pursuit of such a court order is a rights holder's sole remedy in that context. It is vitally important to MasterCard that it not face a claim from a rights holder for failing to take action on a rights holder's notice when the rights holder has an ability to seek a court order against the allegedly infringing site and has the ability to enforce the bill against a payment network provider that has received a copy of the court order and not fulfilled its obligations under the bill related to the court order.

Duty to Monitor. The bill requires a payment network provider to take action based on court orders obtained by the Attorney General and modifications to those court orders. However, the bill currently provides no explicit mechanism for payment network providers to receive notification of modified orders. This gap in the process should be remedied. Also, the bill requires a payment network provider that has acted on a court order obtained by a rights holder

to also take actions based on any subsequent notice from a rights holder that its service is being used to complete payment transactions with an allegedly infringing merchant that was the subject of the order. MasterCard believes that modification of a court order should be a condition to further payment network provider action in the case of a rights holder, as it is in the case of the Attorney General.

Designated Agent Information. The bill contemplates that payment network providers would designate an agent to receive notifications from rights holders, and that the agent's contact information must be posted on the publicly accessible portion of the provider's Internet site. The requirement to post the name and other identifying information of a designated agent creates unnecessary personal risk for individuals designated as agents. The purpose of this requirement could be accomplished through a requirement to have a designated but non-personally identifiable e-mail address that is monitored by the payment network provider. A designated but non-personally identifiable e-mail address is consistent with current industry practice, reduces the potential for process disruption following personnel changes, and eliminates the risk of disruptive or threatening actions being taken against a named agent.

Coverage; Description of Relationship Among the Parties. Other areas of concern include ensuring that the "payment network provider" definition in the bill is sufficiently broad to cover all payment networks. We are confident that this is the intention of the Committee. Also, the bill obligates payment network providers to prevent their systems from being used at infringing Internet sites by persons located in the U.S. and persons subject to the jurisdiction of the U.S. MasterCard is concerned that the latter phrase may require it to determine whether a cardholder located outside of the U.S. is subject to U.S. jurisdiction. Lastly, the framework of the bill contemplates that infringing Internet sites (or merchants more generally) have an account

with a payment network provider. While this may be true of three-party payment networks, it does not accurately describe the relationship of the parties in a four-party payment network, such as MasterCard. We believe that all of these concerns can be addressed in a manner consistent with the intent of the bill.

Conclusion

MasterCard is proud of the role we play and the successes we continue to achieve in combating Internet-related intellectual property infringement. With the collective efforts and commitment of all commercial participants in this fight, we believe that we can forcefully tackle the problem of online piracy of U.S. intellectual property. The Committee's efforts represent an important step in developing a comprehensive framework for addressing this issue and we commend the Committee for its efforts and attention to this matter.

I appreciate the opportunity to appear before you today and I will be glad to answer any questions you may have.

APPENDIX A

MasterCard Worldwide
2000 Purchase Street
Purchase, NY 10577-2509

tel 1 914 249 2000
www.mastercard.com

MasterCard Worldwide

MasterCard Anti-Piracy Policy

The purpose of this document is to set forth MasterCard's policy for addressing the online sale by a Merchant of copyright-infringing products and counterfeit trademark products (the "Anti-Piracy Policy"). The Anti-Piracy Policy supports and is considered in conjunction with MasterCard's Business Risk Assessment and Mitigation ("BRAM") program. The BRAM program, among other things, prohibits a Merchant from submitting for payment, and an Acquirer from accepting from a Merchant for submission for payment, to the MasterCard network any transaction that is illegal, or is deemed by MasterCard in its sole discretion, to damage or have the potential to damage the goodwill of MasterCard or reflect negatively on the MasterCard brand. The following activities are prohibited under the BRAM program: the sale or offer of sale of a product or service other than in full compliance with all laws applicable to the Acquirer, Issuer, Merchant, Cardholder, Cards, or MasterCard (as these terms are defined in the MasterCard Rules).

MasterCard addresses intellectual property piracy as follows:

1 – Law Enforcement Involvement

When a law enforcement entity is involved in the investigation of the online sale of a product or service that allegedly infringes copyright or trademark rights of another party ("Illegitimate Product") by a Merchant and provides MasterCard with evidence of illegal activity for MasterCard's use in taking action under this Policy, MasterCard will endeavor to identify the Acquirer that has the relationship with that Merchant. If MasterCard determines that the merchant is accepting MasterCard cards through an existing acquirer relationship, MasterCard will require that the Acquirer investigate the alleged illegal activity and, within two business days, provide a written report to MasterCard setting forth the results of the investigation and any steps taken to address those results. If the Acquirer determines that the Merchant was engaging in the sale of an Illegitimate Product, the Acquirer must take the actions necessary to ensure that the Merchant has ceased accepting MasterCard cards as payment for the Illegitimate Product. If the Acquirer determines that the Merchant was not engaging in the sale of an Illegitimate Product, the Acquirer must provide to MasterCard compelling evidence demonstrating that finding. MasterCard may exercise discretion to afford the Acquirer additional time to complete the Acquirer's obligations set forth herein. If the Acquirer terminates the Merchant, MasterCard will require that the Acquirer list the Merchant in the MasterCard MATCH compliance system of terminated merchants, where applicable, and thereby afford all Acquirers in the MasterCard network notice that the Merchant has been terminated and of the Reason Code used by the Acquirer for the termination.

2 – No Law Enforcement Involvement

When there is no law enforcement involvement, an intellectual property right holder may notify MasterCard of its belief that the online sale of a product(s) violates its intellectual property rights and request that MasterCard take action upon such belief. MasterCard maintains the following email address for this purpose: ipinquiries@mastercard.com. The notification and request (the "Request") must include:

(a) a description of the alleged infringement, including the specific identity of the site allegedly engaged in the sale of the alleged Illegitimate Product and compelling evidence substantiating the allegation. The notification must specifically identify any products alleged to be an Illegitimate Product and the location of the alleged Illegitimate Product(s) on the website;

(b) evidence that the allegedly Illegitimate Products can be purchased using a MasterCard-branded payment card, for example, by providing a screenshot of the MasterCard logo appearing on the Merchant website. Test transactions are helpful, but not required to submit a complete notification;

(c) a copy of the right holder's cease and desist letter or Digital Millennium Copyright Act (DMCA) notice notifying the website operator or Merchant that it is engaging in infringing activity, or an attestation that, to the best of the right holder's knowledge, the site is not licensed or otherwise authorized to sell the alleged Illegitimate Products in question; and

(d) evidence demonstrating that the right holder owns the copyright(s) or trademark(s) in question.

MasterCard will accept a Request from, and otherwise coordinate with, a trade association with legal authority to act on behalf of an intellectual property right holder. By the submission of the Request, the submitter certifies that (i) the information set forth in the Request is true and accurate to the best of the submitter's knowledge, (ii) MasterCard may disclose the identity of the submitter and the contents of the Request to any person MasterCard deems appropriate, and (iii) the submitter will cooperate in any judicial or other process concerning MasterCard's receipt and use of the information set forth in the Request.

When MasterCard receives a Request, MasterCard will endeavor to identify the Acquirer that has the relationship with that Merchant. If MasterCard determines that the merchant is accepting MasterCard cards through an existing Acquirer relationship, MasterCard will send the Request to the Acquirer and require that the Acquirer investigate the alleged illegal activity and, within five business days, provide a written report to MasterCard setting forth the results of the investigation and any steps taken to address those results. If the Acquirer determines that the Merchant was engaging in the sale of an Illegitimate Product, the Acquirer must take the actions necessary to ensure that the Merchant has ceased accepting MasterCard cards as payment for the Illegitimate Product. If the Acquirer determines that the Merchant was not engaging in the sale of an Illegitimate Product, the Acquirer must provide MasterCard compelling evidence demonstrating that finding. MasterCard may exercise discretion to afford the Acquirer additional time to complete the Acquirer's obligations set forth herein. Following receipt of the results of the Acquirer's investigation, MasterCard will inform the right holder or trade association of those results. If the Acquirer terminates the Merchant, MasterCard will require that the Acquirer list the Merchant in the MasterCard MATCH compliance system of terminated merchants, where applicable, and thereby afford all Acquirers in the MasterCard network notice that the Merchant has been terminated and of the Reason Code used by the Acquirer for the termination.

3 – Other

If the Merchant is located in a country where the online sale of the alleged Illegitimate Product does not violate applicable country laws, the Acquirer must suspend or terminate acquiring sales by that Merchant to account holders of accounts issued in countries where the sale of the alleged Illegitimate Product is illegal or is otherwise prohibited by local law.

4 – Failure to Comply with this Anti-Piracy Policy

MasterCard has the right to limit, suspend, terminate or condition the Membership, Membership privileges, or both, of any Acquirer that MasterCard deems does not comply with applicable law or with this Anti-Piracy Policy. MasterCard has the sole right to interpret and enforce this Anti-Piracy Policy. Furthermore, MasterCard may assess any Acquirer that MasterCard deems does not comply with this Anti-Piracy Policy, as such Policy may be amended from time to time.

219485.5

Mr. SMITH. Thank you, Ms. Kirkpatrick.
And, Ms. Oyama?

TESTIMONY OF KATHERINE OYAMA, COPYRIGHT COUNSEL, GOOGLE, INC.

Ms. OYAMA. Thank you. Chairman Smith, Ranking Member Conyers, Members of the Committee, thank you so much for the opportunity to testify today, not just on behalf of Google, but also on behalf of the Consumer Electronics System Association, CCIA, Net

Coalition, TechNet, and Tech America, which together represents thousands of companies.

Google takes the problem of online piracy and counterfeiting very seriously. We devote our best engineering talent and tens of millions of dollars every year to fight it. In the last year alone, we have spent more than $60 million to weed out bad actors from our ad services. We have shut down nearly 150,000 adware accounts, mostly based on our own detection efforts. And so far, this year, we have processed 5 million DMCA takedown requests, targeting nearly 5,000,000 items.

We are as motivated as anyone to get this right, but the Stop Online Piracy Act is not the right approach. SOPA undermines the legal, commercial, and cultural architecture that has propelled the extraordinary growth of Internet over the past decade, a sector that has grown to $2 trillion in annual U.S. GDP, including $300 billion from online advertising.

Virtually every major Internet company from Twitter to Facebook, Yahoo and eBay, as well as a diverse array of other groups from venture capitalists, to librarians, to musicians, have expressed serious concerns about this bill. Unfortunately, this legislation is overbroad. It undermines the Digital Millennium Copyright Act, which has, for more than a decade, struck a balance. The DMCA provides copyright owners with immediate recourse when they discover infringement online, while also giving service providers the certainty that they need to investigate in the products on which America, millions of Americans rely.

The bill sweeps in and it will send websites that have violated no law. It imposes harsh and arbitrary sanctions without due process.

The following example shows how the bill, as currently written, would work. Imagine a website—let us call it Dave's Online Emporium, which enables small businesses to sell clothing and accessories. More than 99 percent of the sellers on Dave's Emporium are entirely legitimate, but unbeknownst to Dave, one seller has started selling counterfeit bags and T-shirts that parity a copyrighted design. Dave's Emporium takes great care to comply with copyright laws, including takedown procedures, including repeat infringement provisions of the DMCA. But, under the Stop Online Piracy Act, the entire site could be deemed "dedicated to theft." Based on the violations of this single seller, the whole business effectively shut down. Just about any private party—a corporation, the copyright troll, someone with an ax to grind—could send a notice to payment and advertising companies to terminate services to the site without first involving law enforcement were triggering any judicial process. The complaining party has no duty to contact Dave's Emporium directly to resolve the issue before going straight to ads and payment services to terminate his service. If the emporium fails to respond with a counter notice, within 5 days, Dave's site could effectively be put out of business.

Facing these potential risks, Dave might think twice about establishing his online Emporium in the first place. Countless websites of all kinds, commercial, social, personal, could be shuttered or put out of business, based on allegations that may or may not be valid, and the resulting cloud of legal uncertainty would threaten new in-

vestment, entrepreneurship, and innovation. In a new study of venture capitalists, released today, more than 80 percent said that the safe harbor provisions of digital copyright laws are essential. Weakening those safe harbor provisions would have a recession like impact on new investment. And at the same time, this proposal imposes new and unclear obligations on Internet service providers to take "technically feasible and reasonable measures to block access to sites, to remove them from search results, turning these providers into de facto web censors."

This will not work. As long as there is money to be made pushing pirated and counterfeit products, tech savvy criminals around the world will find ways to sell these products online, and ordering ISPs and search engines to disappear websites from the Internet will not change this fundamental reality. We urge you, instead, to target the problem at the source. Shut down illegal foreign sites by cutting off their revenue. We support legislation that builds on the DMCA. Our proposal would empower the Justice Department to target foreign sites that violate current law, and the court could send out order, advertisers and payment services in which our services would be included, to cut off ads and payments to those sites. Google has been working with the Committee on such a solution for over 6 months, and we will continue to do so.

When all is said and done, we must address online piracy effectively in ways that continue to allow the Internet to drive this economy and this country forward. Thank you.

[The prepared statement of Ms. Oyama follows:]

Google™

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

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

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

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

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

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

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

---

[1] McKinsey Global Institute, "Internet Matters," (May 2011), *available at:* http://www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf.
[2] John Dreighton and John Quelch, "Economic Value of the Advertising-Supported Internet Ecosystem," (June 2009) *available at:* http://www.iab.net/insights_research/530422/economicvalue.

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

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

The Problem of Foreign Rogue Sites

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

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

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

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

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

Our Concerns about SOPA

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

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

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

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

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

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

SOPA Would Conflict with and Undermine the DMCA

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

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

SOPA undermines the DMCA safe harbors in three important ways.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SOPA Raises Serious First Amendment Concerns

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

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

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

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

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

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

Toward a Consensus Approach to Fighting Foreign Rogue Sites

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

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

Google's Efforts to Battle Copyright Infringement and Counterfeiting

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

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

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

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

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

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

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

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

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

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

Principles for a Consensus Solution

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

(1) Policymakers should aim squarely at the "worst of the worst" foreign websites without ensnaring legitimate technologies and businesses. At a minimum, this means tailoring the definitions to capture only sites that are violating the law and operating outside the DMCA safe harbors.

(2) New legislation should not alter common law secondary liability principles or undermine the DMCA.

(3) The DMCA strikes the right balance for search engines.

(4) Legislation should not interfere with the health and stability of the Internet, particularly with regard to the DNS.

(5) Policymakers should foreclose private rights of action and tailor intermediary requirements appropriately.

(6) Policymakers should dismantle barriers to encourage greater proliferation of compelling, legal offerings for copyrighted works online.

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

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

Conclusion

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

Attachment: Internet Companies Letter on SOPA

November 15, 2011

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

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

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

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

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

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

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

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

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

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

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

Thank you in advance for your consideration.

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

Mr. SMITH. Thank you, Ms. Oyama.
Mr. Almeida?

TESTIMONY OF PAUL ALMEIDA, PRESIDENT, DEPARTMENT FOR PROFESSIONAL EMPLOYEES (DPE), AMERICAN FEDERATION OF LABOR, CONGRESS OF INDUSTRIAL ORGANIZATIONS (AFL-CIO)

Mr. ALMEIDA. Good morning Chairman Smith, Ranking Member Conyers, and distinguished Members of the Committee. My name is Paul Almeida. I'm the President of the Department for Professional Employees (DPE), a coalition of 22 national unions affiliated with the AFL-CIO. I am honored to speak today on behalf of the 4 million professional and technical people whom our affiliated unions represent. Those people include creators, performers, and crafts people in arts and entertainment and media, professional and technical people in education, health care, and public administration, in aerospace, and other manufacturing, and pharmaceuticals, science, engineering, information, and in professional sports.

The people I represent work in a wide range of occupations and industries. They share a wide range of interests as workers and consumers, as well as ardent defenders of the First Amendment. On their behalf, permit me to commit you and thank you. Their unions unanimously support the Stop Online Piracy Act, as does the entire AFL-CIO.

My message is simple. It has three parts. First, strengthening protections for U.S. intellectual property helps American workers, jobs, incomes, and benefits. Second, counterfeit goods endanger danger, workers, both as workers and consumers. Third, there is no inconsistency between protecting free speech and an open Internet and safeguarding intellectual property. If the United States allows attacks on intellectual property to get an answer, it puts good livelihoods at risk.

Online access continues to accelerate and expand. It increasingly displaces traditional models for distributing content and, thus, heightens the potential for digital theft. Estimates of the number of jobs lost to digital theft in arts, entertainment, and media sector alone run in the hundreds of thousands. Losses of income arise because entertainment professionals depend on compensation at two points—first, when the professionals do the work, and later with the reuse of the intellectual property. Royalties and residuals from downstream revenues enable entertainment professionals to survive between projects.

In manufacturing, the estimates of losses from counterfeits also run in the billions. Again, the victims include workers who face lost jobs and income. We should not allow rogue websites to facilitate the distribution of counterfeit goods.

My second point, counterfeits endanger workers as workers and as consumers. Only last week, the Senate Committee on Armed Services heard about an astonishing extent of counterfeit electronic parts in the military supply chain. Counterfeits kill. When protective vests are fake, soldiers and police officers can die. When prescription drugs are fake, patients can die. And when smoke detectors are fake, home owners and firefighters can die.

In May, the Atlanta, Georgia, Fire and Rescue Department recalled roughly 18,500 smoke detectors that it distributed for a free Atlanta smoke alarm program. The smoke detectors were counter-

feit, and so were the underwriter laboratory seals. An alert from the U.S. Consumer Product Safety Commission noted, "The unreliable, counterfeit alarms pose a life safety hazard to the occupants in the event of a fire."

Counterfeit smoke detectors pose a life safety hazard, not just home owners, but to firefighters. Harold Schaitberger, General President of the International Association of Firefighters, another union affiliated with DPE, wrote to Chairman Smith and Ranking Member Conyers to support the Stop Online Piracy Act. President Schaitberger noted that, "The preparedness and safety of our members depends on reliable equipment." A blog called TechKnit.com posted a defamatory response. "Who does the MPAA actually think it is fooling? Is Congress so stupid that it cannot figure out for itself that firefighters have no clue what the debate is about?" The blog accused firefighters of supporting censorship. It implied the only reason the firefighters spoke up was because the MPAA was paying off the union. Firefighters know the consequences of counterfeit equipment.

My third point, freedom of speech is not the same as lawlessness on the Internet. Protecting intellectual property is not the same as censorship. The First Amendment does not protect stealing goods off trucks. I mentioned earlier that the people whom I represent today include ardent defenders of the First Amendment, newspaper and broadcast journalists, radio broadcasters, news writers, script writers, and many others in the arts and entertainment and media. When they oppose wage theft, there is no inconsistency with the First Amendment.

Digital theft and rogue websites diminishes incentives to invest, and leads to a downward spiral for U.S. workers in our economy. That is the bad news. The good news is that you are taking action. The professional and technical workers and their unions whom I represent look forward to your passing the Stop Online Piracy Act.

Thank you.

[The prepared statement of Mr. Almeida follows:]

WRITTEN STATEMENT OF
PAUL E. ALMEIDA,
PRESIDENT,
DEPARTMENT FOR PROFESSIONAL EMPLOYEES, AFL-CIO

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

on

H.R. 3261, THE "STOP ONLINE PIRACY ACT"

November 16, 2011

Good morning, Chairman Smith, Ranking Member Conyers, and distinguished Members of the Committee. My name is Paul Almeida. I am the President of the Department for Professional Employees (DPE), a coalition of 22 national unions affiliated with the AFL-CIO. I have listed those unions at the end of this written statement. I am honored to speak today on behalf of the more than four million professional and technical people whom our affiliated unions represent.

Those people include creators, performers, and craftspeople in the arts, entertainment, and media: writers, broadcast journalists, singers and musicians, stage employees, actors, and many more. They include professional and technical people in education, health care, and public administration; in aerospace and other manufacturing sectors; in pharmaceuticals, science, engineering, and information technology; and in professional sports. In these times of high unemployment and economic crisis, their occupations range across several of the most vibrant sectors of the U.S. economy. These are sectors where professional and technical people – seeking the ability to do their jobs right – have organized into unions in large numbers; where creativity and ingenuity propel success; and where, unlike other segments of the economy, industries like aerospace and entertainment enjoy a trade surplus.

Just as the people I represent work in a wide range of occupations and industries, they bring to the Stop Online Piracy Act a wide range of interests: as workers and consumers as well as ardent defenders of the First Amendment. On their behalf, permit me to commend and thank you. Many of you have worked on a bipartisan basis with business and labor over many years to combat digital theft, piracy of intellectual property, and counterfeiting. I am pleased to acknowledge your expertise and

effectiveness. The unions that the professional and technical people whom I represent have organized unanimously support the Stop Online Piracy Act.

Their strong support has brought the support of the entire AFL-CIO, 12.2 million workers in 57 national and international unions. In May, AFL-CIO President Richard Trumka applauded the introduction of the PROTECT IP Act, S. 968, in the Senate. His words apply equally to the Stop Online Piracy Act: "The economic well-being of workers in the United States – jobs, income, and benefits – turns more and more on our protecting the creativity and innovation that yield world-class entertainment, cutting-edge and sustainable manufacturing and construction, and disease-ending pharmaceuticals. In a tough economic time, [this legislation] will help to protect U.S. workers and consumers against digital thieves and counterfeit scammers." President Trumka's statement followed a unanimous AFL-CIO Executive Council statement in March 2010, "Piracy is a Danger to Entertainment Professionals," that is attached to my written testimony below.

My message is simple. It has three parts. First, strengthening protections for U.S. intellectual property helps American workers, jobs, incomes, and benefits. Theft of intellectual property raises unemployment and cuts income.

Second, counterfeit goods endanger workers, both as workers and as consumers.

Third, freedom of speech is not the same as lawlessness on the Internet. There is no inconsistency between protecting an open Internet and safeguarding intellectual property.

Start with American workers, jobs, incomes, and benefits. A May 2011 report from the U.S. International Trade Commission focused on China, its infringement on U.S. intellectual property rights, and American jobs. The report estimated conservatively

that if China enforced intellectual property rights as the United States does, U.S. firms operating in China would add "approximately 923,000 new jobs" in the United States. A second, less conservative forecast foretold an increase of 2.1 million jobs – and please remember, this report focused on China alone.

For too many workers in the United States today, jobs, income, and benefits are hard to come by. If the United States allows attacks on intellectual property to go unanswered, it puts good livelihoods at risk.

Online access continues to accelerate and expand. It increasingly displaces traditional models for distributing content and thus heightens the potential for digital theft. High-speed broadband has, for example, enabled illegal online streaming of television shows, films, and sports events.

Among the unions affiliated with the Department for Professional Employees are nine representing creators, performing artists, and craft workers. Those unions include the Actors' Equity Association, the American Federation of Musicians, the American Federation of Television and Radio Artists, the American Guild of Musical Artists; the International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts; the International Brotherhood of Electrical Workers, the Office and Professional Employees International Union, the Screen Actors Guild, and the Writers Guild of America, East.

As I testified before the Senate Judiciary Committee last year, estimates of the number of jobs lost to digital theft *in the arts, entertainment, and media sector alone* run to the hundreds of thousands. While exact numbers are difficult to find, there can be no

question about the magnitude of the problem for the entire United States: billions of dollars in lost revenues for U.S. industries and millions of lost U.S. jobs.

Losses of income arise because entertainment professionals depend on compensation at two points: first when the professionals do the work, and later when others use and reuse the intellectual property that the professionals created. Royalties and residuals from downstream revenues enable entertainment professionals to survive between projects.

A second example is manufacturing. Among the unions affiliated with the Department for Professional Employees are the International Association of Machinists and Aerospace Workers, the International Brotherhood of Electrical Workers, the International Federation of Professional and Technical Engineers, and the United Steelworkers. Again, the estimates of losses from counterfeiting run to billions of dollars. Again, the victims include workers, who face lost jobs and income. From auto parts to circuit breakers, counterfeiting endangers all of us with unreliable products. We should not allow rogue websites to facilitate the distribution of counterfeit goods.

Only last week the Senate Committee on Armed Services heard about the astonishing extent of counterfeit electronic parts in the military supply chain. Counterfeits taint the original products with their inferior quality. More important, counterfeits kill. When brakes are fake, drivers die. When prescription drugs are fake, patients die. When protective vests are fake, soldiers and police officers die. And when smoke detectors are fake, homeowners and firefighters die.

This is my second point. Counterfeits endanger workers, as workers and as consumers.

Permit me to share one example of many. In May, the Atlanta, Georgia Fire Rescue Department recalled roughly 18,500 smoke detectors that it distributed for free since 2006 as a part of the Atlanta Smoke Alarm Program. The smoke detectors were counterfeit. So too were the Underwriters Laboratories seals on the smoke detectors.

The vendors of the counterfeit smoke detectors had attributed initial delays in delivering the counterfeits to the Chinese New Year. Investigation by a local broadcast journalist revealed that the vendors served prison time for selling counterfeit smoke detectors to the federal government and were banned from doing business with it.

An alert about the smoke detector recall from the U.S. Consumer Product Safety Commission on May 27 noted: "Some alarms did not respond within an adequate time for life safety and other alarms did not respond at all." It concluded that the alarms "pose a life safety hazard to the occupants in the event of a fire."

Counterfeit smoke detectors pose "a life safety hazard" not just to homeowners, but to firefighters. Delays when a fire begins mean the fire may rage out of control. In September, Harold A. Schaitberger, General President of the International Association of Fire Fighters, another union affiliated with the Department for Professional Employees, wrote to Chairman Smith, Ranking Member Conyers; Subcommittee on Intellectual Property, Competition, and the Internet Chairman Goodlatte and Ranking Member Watt; as well as Senators Leahy and Grassley, to support the PROTECT IP Act and companion legislation in the House. In President Schaitberger's words, "The preparedness and safety of our members depend on sound, reliable equipment."

President Schaitberger also observed that rogue websites deprive local governments of much needed taxes: "lost tax revenue means fewer police officers and

firefighters." I would like to underscore that point. Criminal syndicates in Russia are unlikely to pay federal, state, or local taxes. They generally prefer the Al Capone model.

Unfortunately, this story does not end with President Schaitberger's letter. A blog titled techdirt.com this month attacked the International Association of Fire Fighters for striving to keep consumers and firefighters safe. Permit me to quote directly from the post:

> What are the chances that the International Association of Fire Fighters has received large checks from those associated with the movie business? But, more seriously, who does the MPAA actually think it's fooling? Is Congress so stupid that it can't figure out for itself that firefighters have no clue what this debate is about? Otherwise, why would they be supporting censorship in America?

This defamatory blast brings me to my third point: Freedom of speech is not the same as lawlessness on the Internet. There is no inconsistency between protecting an open Internet and safeguarding intellectual property. Protecting intellectual property is not the same as censorship; the First Amendment does not protect stealing goods off trucks. In the words of First Amendment advocate and expert Floyd Abrams, "It is one thing to say that the Internet must be free; it is something else to say that it must be lawless."

Those words come from an analysis that three unions affiliated with the Department for Professional Employees – the American Federation of Television and Radio Artists, the International Alliance of Theatrical Stage Employees, and the Screen Actors Guild – in combination with the Directors Guild of America and the Motion Picture Association asked Mr. Abrams to undertake. Noting that the Internet is subject to

the same principles of libel, privacy, and copyright that govern other media, Mr. Abrams concluded that the Stop Online Privacy Act "is consistent with the First Amendment." As the Supreme Court declared, "copyright supplies the economic incentive to create and disseminate ideas." H.R. 3261, Mr. Abrams wrote, "would protect creators of speech, as Congress has done since this Nation was founded, by combating its theft." (Letter of November 7, 2011 to Chairman Smith and Ranking Member Conyers from Floyd Abrams, Esquire.)

I mentioned earlier that the people whom I have the honor to represent today include ardent defenders of the First Amendment. They work as newspaper journalists, broadcast journalists, radio broadcasters, news writers, scriptwriters, and in many other aspects of the arts, entertainment, and media. When they oppose wage theft, they see no inconsistency with the First Amendment.

In June, the Writers Guild of America East hosted a briefing in the U.S. Senate Committee on the Judiciary hearing room, "The Internet from the Creators' Perspective." The Writers Guild message had two parts: Keep the Internet open, and fight digital theft. None of the presenters saw the two parts as inconsistent. Nor do I. Nor does Secretary of State Hillary Rodham Clinton. In an October 25, 2011 letter to Representative Howard L. Berman, she declared that the State Department "is strongly committed to advancing both Internet freedom and the protection and enforcement of intellectual property rights on the Internet" – priorities that are not contradictory, but consistent.

In April, the Department for Professional Employees highlighted this same consistency at a White House meeting about Internet policy in the Organisation for Economic Co-operation and Development:

We view our support for the unfettered flow of information as distinct from suggesting that all content on the Internet should be available without cost to the consumer. Permitting digital theft and other violations of intellectual property rights will lead to less rather than more economic growth, and to a poorer, less creative rather than more vibrant Internet.

The consequences from digital theft and rogue websites include a diminished incentive to invest and a downward spiral for U.S. workers and our economy. That's the bad news. The good news is that you are taking action. On behalf of the professional and technical workers and their unions whom I have the honor to represent, I look forward to your passing the Stop Online Piracy Act into law.

Thank you for inviting me to participate in this hearing. I would be happy to answer any questions you may have.

Unions Affiliated with the Department for Professional Employees, AFL-CIO

Actors' Equity Association (AEA)
American Federation of Government Employees (AFGE)
American Federation of Musicians (AFM)
American Federation of School Administrators (AFSA)
American Federation of Teachers (AFT)
American Federation of Television and Radio Artists (AFTRA)
American Guild of Musical Artists (AGMA)
Federation of Professional Athletes (FPA)
International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts (IATSE)
International Association of Fire Fighters (IAFF)
International Association of Machinists and Aerospace Workers (IAM)
International Brotherhood of Electrical Workers (IBEW)
International Federation of Professional and Technical Engineers (IFPTE)
International Plate Printers, Die Stampers and Engravers Union of North America
International Union of Painters and Allied Trades (IUPAT)
Office and Professional Employees International Union (OPEIU)
Retail, Wholesale and Department Store Union (RWDSU)
Screen Actors Guild (SAG)
Seafarers International Union of North America (SIU)
United Steelworkers (USW)
Utility Workers Union of America (UWUA)
Writers Guild of America, East (WGAE)

AFL-CIO Executive Council Statement
Orlando, Florida
March 2, 2010

PIRACY IS A DANGER TO ENTERTAINMENT PROFESSIONALS

Submitted by the Department for Professional Employees, AFL-CIO (DPE) for the Arts, Entertainment and Media Industries Unions Affiliated with DPE

Motion pictures, television, sound recordings and other entertainment are a vibrant part of the U.S. economy. They yield one of its few remaining trade surpluses. The online theft of copyrighted works and the sale of illegal CDs and DVDs threaten the vitality of U.S. entertainment and thus its working people.

The equation is simple and ominous. Piracy costs the U.S. entertainment industry billions of dollars in revenue each year. That loss of revenue hits directly at bottom-line profits. When profits are diminished, the incentive to invest in new films, television programs, sound recordings and other entertainment drops. With less investment in future works comes less industry activity that directly benefits workers: fewer jobs, less compensation for entertainment professionals and a reduction in health and pension benefits.

Combating online theft and the sale of illegal CDs and DVDs is nothing short of defending U.S. jobs and benefits. In the case of music, experts estimate that the digital theft of sound recordings costs the U.S. economy $12.5 billion in total output and costs U.S. workers 71,060 jobs.[1] In the motion picture industry, piracy results in an estimated $5.5 billion in lost wages annually, and the loss of an estimated 141,030 jobs that would otherwise have been created.[2]

Illegal CDs and DVDs have afflicted even live theatre. Websites sell illegal DVDs of Broadway shows, which reduces sales of tickets and authorized CDs and DVDs. Selling illegal CDs or DVDs of plays, musicals and other shows not only steals the work of the entertainment professionals, but makes quality control impossible.

Most of the revenue that supports entertainment professionals' jobs and benefits comes from the sale of entertainment works including sales in secondary markets—that is, DVD and CD sales, legitimate downloads, royalties and, in the case of TV shows or films, repeated airings on free cable or premium pay television. Roughly 75 percent of a

---

[1] Siwek, Stephen. (8/21/07). *The True Cost of Sound Recording Piracy to the U.S. Economy*. Retrieved from: http://www.ipi.org/IPI/IPIPublications.nsf/PublicationLookupFullText/5C2EE3D2107A4C228625733E0053A1F4

[2] Siwek, Stephen. (9/20/06). *The True Cost of Sound Recording Piracy to the U.S. Economy*. Retrieved from: http://www.ipi.org/IPI/IPIPublications.nsf/PublicationLookupFullText/E274F77ADF58BD08862571F8001BA6BF

motion picture's revenues comes after the initial theatrical release, and more than 50 percent of scripted television production revenues are generated after the first run.

In most work arrangements, a worker receives payment for his or her effort at the completion of a project or at set intervals. The entertainment industry, however, operates on a longstanding unique business model in which compensation to workers—pay and benefit contributions—comes in two stages. Film, television and recording artists, as well as film and television writers, receive an initial payment for their work and then residuals or royalties for its subsequent use. Those payments also generate funds for their health and pension plans. The below-the-line workers, the craft and technical people who manage equipment, props, costumes, makeup, special effects and other elements of a production, also receive compensation for their work, while payment for subsequent use goes directly into their health and pension plans.

Motion picture production is a prime example. The professionals involved with the initial production of a film—the actors who perform, the craftspeople behind the scenes, the musicians who create the soundtrack and the writers who craft the story—each receive an initial payment for their work. When that work is resold in the form of DVDs or CDs, or to cable networks or to airlines or in foreign sales, a portion of these "downstream revenues" are direct compensation to the film talent or recording artists who were involved in those productions or recordings.

These residuals help keep entertainment professionals afloat between projects. Entertainment professionals may work for multiple employers on multiple projects and face gaps in their employment. Payment for the work they have completed helps sustain them and their families through underemployment and unemployment. For AFTRA recording artists in 2008, 90 percent of income derived from sound recordings was directly linked to royalties from physical CD sales and paid digital downloads. SAG members working under the feature film and TV contract that same year derived 43 percent of their total compensation from residuals. Residuals derived from sales to secondary markets funded 65 percent of the IATSE MPI Health Plan and 36 percent of the SAG Health and Pension Plan. WGAE-represented writers often depend on residual checks to pay their bills between jobs; in some cases, the residual amounts can be as much as initial compensation. Online theft robs hard-earned income and benefits from the professionals who created the works.

There are tools that can be used to fight digital piracy. Internet service providers (ISPs) have the ability to find illegal content and remove or limit access to it. To be truly effective, these sanctions must depart from the costly and ineffective legal remedies traditionally employed to counter theft of copyrighted material. The European Union is developing and implementing model policies for which the trade union movement is providing strong and critical support. These policies illustrate that there are answers that make sense in a digital age.

At the core of any effort to combat digital theft is reasonable network management, which should allow ISPs to use available tools to detect and prevent the illegal downloading of copyrighted works. With respect to lawfully distributed content, ISPs should not be allowed to block or degrade service so that both consumers and copyright would be protected.

The unions of the AFL-CIO that represent professionals in the Arts, Entertainment and Media Industries (AEMI) include Actors' Equity Association (AEA), the American Federation of Musicians (AFM), the American Federation of Television and Radio Artists (AFTRA), the American Guild of Musical Artists (AGMA), the International Alliance of Theatrical Stage Employes, Moving Picture Technicians, Artists and Allied Crafts (IATSE), the International Brotherhood of Electrical Workers (IBEW), the Office and Professional Employees International Union (OPEIU), the Screen Actors Guild (SAG) and the Writers Guild of America, East (WGAE). The AEMI unions are wholly in support of the widest possible access to content on the Internet and the principles of net neutrality, so long as intellectual property rights—and the hundreds of thousands of jobs that are at stake—are respected.

Some would like to portray the debate over Internet theft as one in which a few wealthy artists, creators and powerful corporations are concerned about "giving away" their "product" because they are greedy and cannot change with the times to create new business models. The hundreds of thousands of people represented by the AEMI unions of the AFL-CIO are a testament to the falsity of that proposition.

Online theft and the sale of illegal CDs and DVDs are not "victimless crimes." Digital theft costs jobs and benefits. It is critical, at this important moment in the evolution of the Internet and potential Internet policy, for union members and leaders to publicly and visibly engage in a sustained effort to protect members' livelihoods, the creation and innovation that are the hallmark of their work and the economic health and viability of the creative industries in this country. The AEMI unions and other unions in U.S. entertainment stress that pirated content is devastating to the entertainment professionals who create the underlying works.

The AFL-CIO strongly supports the efforts of the AEMI unions and the Department for Professional Employees, AFL-CIO, to combat piracy. It commends their work with government and industry to develop workable solutions to protect the interests of their members. The AFL-CIO urges its affiliate unions to educate their members about the adverse impact of piracy; to support efforts to ensure that government officials and lawmakers are aware of, and support the protection of, entertainment industry jobs that will be lost to online theft; to encourage their members to respect copyright law; and to urge their members, as a matter of union solidarity, to never illegally download or stream pirated content or purchase illegal CDs and DVDs.

# # #

Mr. SMITH. Thank you, Mr. Almeida.

I will recognize myself for questions. And, Ms. Pallante, let me direct a couple of questions to you.

In your prepared a written statement, you said, "If Congress does nothing to provide serious responses to online piracy, the U.S. copyright system will ultimately fail." What did you mean by that?

Ms. PALLANTE. Thank you, Mr. Chairman. Yes, I do not think that is an overstatement. The system that we have for copyright and have had since 1790, is based on a system of exclusive rights with which authors can license and which publishers and producers can invest in, and then distribute and otherwise bring to life for consumers, not only here, but through reciprocal agreements with foreign countries.

If those exclusive rights cannot be meaningfully enforced and can be usurped in a lawless environment, they will become meaningless. And if Congress does not update the piracy laws, as it has done consistently for many, many years, many decades, hundreds of years——

Mr. SMITH. I think you just anticipated my next question, which was going to be, do you think the legal system has all the tools it needs now to combat the infringing websites?

Ms. PALLANTE. I do not. I think that this is a timely hearing. I think Congress has done an excellent job of intervening when technology outpaces the law. It did that in the Net Act. It did that in the Art Act. And I think that this is similar legislation. We are looking at a situation where very sophisticated and very smart and very blatant infringers will leap to offshore locations so that they can direct infringing goods, which often belong to our companies, back to American consumers. They are outside the jurisdiction of our courts. We are not suggesting that we would intervene in domestic courts in foreign countries. What we are saying is that we should have some response to allowing them to do that with impunity.

Mr. SMITH. Okay. Thank you, Ms. Pallante.

Ms. Oyama, let me direct a couple of questions to you. And, first, let me say that you spoke a lot of the right words today. We have heard those words before, and I only hope that your company and other similar companies will practice what you preached. And that we will wait to see.

Let me ask you a couple of questions. You do acknowledge that there is a severe problem, I gather, with the theft of intellectual property by foreign criminals?

Ms. OYAMA. That is a problem that we take extremely seriously. We have hundreds of employees that work on it.

Mr. SMITH. And I believe you agreed that if we cut off access to American consumers and U.S. dollars, that that will decrease the amount of intellectual property theft as well.

Ms. OYAMA. We think cutting off the money is a very effective solution.

Mr. SMITH. Okay.

Ms. OYAMA. The sites are in business because they profit.

Mr. SMITH. Now, particularly with regard to Google, do you think Google should stop returning search results for foreign sites that are breaking U.S. law?

Ms. OYAMA. Under the Digital Millennium Copyright Act, a rightsholder could come directly to Google. It would not need to go to court, and they could alert us of the foreign infringement. And we remove that.

Mr. SMITH. Well, a lot of people do not think the DMCA is sufficient, including the Register of Copyrights. Do you think we should go beyond that to try to stop returning search results for foreign sites?

Ms. OYAMA. Thank you for the question. I think there is a lot of misperception about what is and what is not——

Mr. SMITH. No, no. I was asking you a specific question here. Should Google stop returning search results for foreign sites that are breaking U.S. law?

Ms. OYAMA. We do when notified by rightsholders. We have done that more than 5 million times.

Mr. SMITH. The answer is yes, then?

Ms. OYAMA. Yes.

Mr. SMITH. Okay, thank you. Another question is this. Should Google stop placing ads on illegal sites that are stealing American intellectual property?

Ms. OYAMA. Our policies prohibit that. We have proactively ejected more than 12,000 sites this year.

Mr. SMITH. Okay. And so, you would agree not to either facilitate or place ads on illegal sites that are stealing U.S. property?

Ms. OYAMA. If a site is violating the law, we would eject them from our system, and we do that.

Mr. SMITH. Again, I hope you can practice what you preach today. That would be a major breakthrough.

It seems to me, and let me just conclude in this way, that Google and other companies really have a decision to make. And I hope they will make the right decision. I hope they will decide to help other American companies. It is not necessarily going to benefit Google or some of your allies, but I hope you will decide to help American companies protect their intellectual property from being infringed by foreign criminals. And that is, I know a decision that you all are having to make and weigh.

I acknowledge and regret to a large extent that if you make the right decision, that is going to mean you are going to have to give up some of the revenue you might get from some of those ads that are actually on the infringing websites themselves. That is a decision for you all to make, but I think you can make the right one there.

I simply hope that you and others will decide to do what is good for other American companies, do what is good for American jobs, and do what is good for the American economy as well. But thank you for your testimony.

The gentleman from California, Mr. Berman, is recognized for 5 minutes.

Mr. BERMAN. Well, thank you very much, Mr. Chairman and Ranking Member Conyers. And I would like to thank the Chairman for responding to my letter inviting Google to testify. I think it is extremely important to understand what legitimate issues the opposition may have, so they can be addressed. I have not heard contrary changes they would recommend. I have not received a Google

proposal or suggested proposal on focusing on foreign rogue websites, and would love to see it since it has apparently been discussed with the Committee.

Opponents of the legislation say we support the bill's stated goals, and asked that sponsors consider more targeted ways to combat foreign rogue websites. That is the response to every idea put forward to stop that. Why is this not the time for the tech community to put forward concrete and specific proposals that will effectively combat the theft that take place on the Internet?

The rhetoric around this bill is over the top. None of the sponsors of this bill are against the First Amendment. None of the sponsors of this bill want to shut down the Internet. And none of the sponsors want to stymie technology. Perhaps the first example that I will focus on is opponents claiming that the legislation will undermine U.S. foreign policy, and encourage repression by foreign governments. I wrote to Secretary Clinton and asked her opinion. She clearly and forcefully said there is no contradiction between intellectual property rights protection and enforcement ensuring freedom of expression on the Internet. In other words, we can adopt legislation like H.R. 3261. To better protect U.S. intellectual property online, at the same time demand that foreign governments respect Internet freedom. And I would like to submit those letters for the record.

Mr. SMITH. Without objection.

[The information referred to follows:]

ILEANA ROS-LEHTINEN, FLORIDA, CHAIRMAN

CHRISTOPHER H. SMITH, NEW JERSEY
DAN BURTON, INDIANA
ELTON GALLEGLY, CALIFORNIA
DANA ROHRABACHER, CALIFORNIA
DONALD A. MANZULLO, ILLINOIS
EDWARD R. ROYCE, CALIFORNIA
STEVE CHABOT, OHIO
RON PAUL, TEXAS
MIKE PENCE, INDIANA
JOE WILSON, SOUTH CAROLINA
CONNIE MACK, FLORIDA
JEFF FORTENBERRY, NEBRASKA
MICHAEL T. MCCAUL, TEXAS
TED POE, TEXAS
GUS M. BILIRAKIS, FLORIDA
JEAN SCHMIDT, OHIO
BILL JOHNSON, OHIO
DAVID RIVERA, FLORIDA
MIKE KELLY, PENNSYLVANIA
TIM GRIFFIN, ARKANSAS
TOM MARINO, PENNSYLVANIA
JEFF DUNCAN, SOUTH CAROLINA
ANN MARIE BUERKLE, NEW YORK
RENEE ELLMERS, NORTH CAROLINA

YLEEM D.S. POBLETE
STAFF DIRECTOR

One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Foreign Affairs
2170 Rayburn House Office Building
Washington, DC 20515
www.hcfa.house.gov

HOWARD L. BERMAN, CALIFORNIA
RANKING DEMOCRATIC MEMBER

GARY L. ACKERMAN, NEW YORK
ENI F.H. FALEOMAVAEGA, AMERICAN SAMOA
DONALD M. PAYNE, NEW JERSEY
BRAD SHERMAN, CALIFORNIA
ELIOT L. ENGEL, NEW YORK
GREGORY W. MEEKS, NEW YORK
RUSS CARNAHAN, MISSOURI
ALBIO SIRES, NEW JERSEY
GERALD E. CONNOLLY, VIRGINIA
THEODORE E. DEUTCH, FLORIDA
DENNIS CARDOZA, CALIFORNIA
BEN CHANDLER, KENTUCKY
BRIAN HIGGINS, NEW YORK
ALLYSON SCHWARTZ, PENNSYLVANIA
CHRISTOPHER S. MURPHY, CONNECTICUT
FREDERICA WILSON, FLORIDA
KAREN BASS, CALIFORNIA
WILLIAM KEATING, MASSACHUSETTS
DAVID CICILLINE, RHODE ISLAND

RICHARD J. KESSLER
DEMOCRATIC STAFF DIRECTOR

September 8, 2011

The Honorable Hillary Clinton
Secretary of State
U.S. Department of State
2201 C Street NW
Washington DC 20520

Dear Secretary Clinton:

I read with great interest your January 21, 2010 speech on internet freedom. It was timely and prescient given the suppression that was to occur on communication media over the course of the Arab Spring. The internet and other social media technologies were invaluable in fostering communication and spreading information as history was being made.

I write to ask that the State Department reaffirm United States foreign policy encompasses both internet freedom and the promotion of strong, effective protection of intellectual property (IP) online. While these two principles can be applied simultaneously, opponents of IP protection have repeatedly mischaracterized your words on this point. They claim that U.S. efforts to stop online IP theft may provide an excuse for regimes that suppress dissent by curtailing internet freedom. These mischaracterizations have been repeated so often, including through paid ads in publications aimed at Members of Congress, that I believe it imperative for the State Department to set the record straight.

One example is a July 5th, 2011 letter[1] to Congress from opponents of the PROTECT IP ACT, which selectively quoted your remarks to support the contention that legislation providing effective protection to IP online "will undermine United States foreign policy and strong support of free expression on the Internet around the world."[2] These selective quotations suggest that U.S. efforts to disrupt the business models of online thieves would constitute the same sort of

---

[1] See Letter from Opponents to the PROTECT IP Act, at http://www.scribd.com/doc/59241037/PROTECT-IP-Letter-Final.

[2] See page 1 of the Letter from Opponents to the PROTECT IP Act.

Internet censorship for which you and the Administration have rightly condemned China, Iran and other nations.

I know that law enforcement, and the rule of law, is a pillar of U.S. foreign policy, and is fully consistent with our promotion of Internet freedom. Indeed, your "Remarks on Internet Freedom" made clear that free expression does not protect "those who use the internet to...distribute stolen intellectual property"[3] - a fact conveniently overlooked by those who mischaracterize that speech. Your view is supported by the noted First Amendment scholar, Floyd Abrams, in his analysis of the legislation.[4] He said that, "as a matter of both constitutional law and public policy, the U.S. must remain committed to defending *both* the *right* to speak and the ability *to protect* one's intellectual creations."

The Internet and recent history, underscore the complexity of the challenge. When despots shut down the Internet to suppress dissent, the U.S. must condemn it. But that does not mean that governments are defenseless against crime and fraud when it is carried out online. You spoke of the urgent need to protect online speech – but also said that "all societies recognize that freedom of expression has its limits," and that those who use the internet to "distribute stolen intellectual property cannot divorce their online actions from their real world identities." President Obama's International Strategy for Cyberspace targeted "the persistent theft of intellectual property" as a key threat to competitiveness and innovation, and vowed that our country "will take measures to identify and respond to such actions, and hold such actors accountable."

I believe that if we can provide an open and transparent judicial process, consistent with due process, that responds to online theft swiftly, surgically and fairly, we set a positive precedent for others to follow. Copyright theft and trademark counterfeiting are illegal in virtually every country of the world. If the US leads the way, it strengthens us when we object to arbitrary actions that shut down a country's communications networks. To pretend that authoritarian regimes will be less likely to abuse their power if the U.S. refrains from adopting new laws against online theft is a fantasy, not a policy.

Law enforcement actions over the past year shows that a civil society need not surrender to lawlessness. In "Operation in Our Sites," Justice and Homeland Security officials acted to cut off websites engaged in counterfeiting and theft, and deny them access to the businesses that

---

[3] See http://www.state.gov/secretary/rm/2010/01/135519.htm, "Now, all societies recognize that free expression has its limits...Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes."

[4] See http://www.dga.org/en/News/PressReleases/2011/0524-Floyd-Abrams-Letter.aspx

facilitated their unlawful online business models. Agents conducted thorough investigations, presented evidence to US Attorneys, and together the federal officers went before a U.S. District Court. With a court order in hand, they have seized some 130 different rogue domain names and in not one case took action against a business with even a colorable claim of legitimacy under U.S. law. In one non-copyright case, a seizure of child sexual abuse sites inadvertently swept in some legitimate online activities. ICE quickly fixed the mistake, and presumably learned from the experience. I am hoping that tech companies – those who understand our goals – help law enforcement ensure that implementation is narrowly tailored and effective.

Assertions that protection of intellectual property on the internet is inconsistent with supporting internet freedom, if continuously repeated and unanswered, have a way of becoming fixed as truth in the minds of many. Therefore, I believe it imperative for the State Department to publicly clarify the misstatements referenced above, and to publicly affirm that our support for Internet freedom does not extend to the freedom to steal intellectual property.

Thank you for your prompt consideration of this request.

Warm Regards,

HOWARD L. BERMAN
Ranking Member

Cc: Undersecretary of State Robert Hormats
Intellectual Property Enforcement Coordinator Victoria Espinel

THE SECRETARY OF STATE
WASHINGTON

October 25, 2011

The Honorable Howard L. Berman
Committee on Foreign Affairs
House of Representatives
Washington, D.C. 20515

Dear Mr. Berman:

Thank you for your letter of September 8 regarding Internet freedom and the relationship between Internet freedom and the protection of intellectual property rights on the Internet.

The State Department is strongly committed to advancing both Internet freedom and the protection and enforcement of intellectual property rights on the Internet. Indeed, these two priorities are consistent. The protection and enforcement of intellectual property rights on the Internet is critical for the United States, for its creators and inventors, and for the jobs it promotes and the economic promise it provides. There is no contradiction between intellectual property rights protection and enforcement and ensuring freedom of expression on the Internet.

We must hold governments accountable to the international commitments and obligations they have undertaken with respect to freedom of expression, which apply equally to online activity. Given the volume of communication over the Internet today, we have focused our efforts on ensuring that the Internet is a medium through which people can safely and effectively express their opinions. The Arab Spring shows the promise of the Internet as a medium by which peaceful demonstrators can mobilize citizens in the face of government oppression. The Internet also offers tremendous opportunity for creators and inventors, but that promise will not be met unless the rules of copyright and trademark are protected and enforced. The rule of law is essential to both Internet freedom and protection of intellectual property rights, which are both firmly embedded in U.S. law and policy.

There will be many opportunities in the future for the State Department to reiterate publicly that Internet freedom and intellectual property protection are mutually consistent. And as those opportunities arise, we will take care to ensure that our international partners understand that our commitment to the rule of law encompasses both online and offline activity. We will also ensure that our international partners understand they must meet their own commitments to Internet freedom and intellectual property protection online, just as they do offline.

We hope that this information is helpful to you. Please do not hesitate to contact us if we can be of further assistance on this or any other matter.

Sincerely yours,

Hillary

Hillary Rodham Clinton

Mr. BERMAN. Based on your answers to Mr. Smith's question, I would like to follow up. I thought I heard you say in response to the Chairman's question that Google does not legal to pirate websites?

Ms. OYAMA. Under the DMCA procedures that Congress set out, a rightsholder can notify Google about foreign infringement, and we would remove that site.

Mr. BERMAN. All right. Well, explain to me this one. The Pirate Bay is a notorious pirate site, a fact that its founders proudly proclaim in the name of the site itself. In fact, the site's operators have been criminally convicted in Europe. One has apparently fled to Cambodia. It is being blocked by court order in at least Italy, Denmark, Belgium, Ireland, and Finland. And yet, Google continues to send U.S. customers, or at least I do not know what you are doing this morning, but before this morning, because maybe you could read my mind. U.S.-Google continues to send U.S. consumers to the site by linking to the site in your search results. Why do you do this, requiring copyright owners to send thousands upon thousands of notices for individual Torrent Links Pirate Bay, only to have those same files reappear on the system, when Google calls The Pirate Bay again? And we all know that this is a notoriously egregious pirate site. Why does Google refuse to de-index the site in your search results?

Ms. OYAMA. Copyright infringement, counterfeiting, these are issues that we take incredibly seriously. We invest tens of millions of dollars into the problem. We have hundreds of people around the world that work on it.

When it comes to copyright——

Mr. BERMAN. Why does Google refuse to de-index the site in your search results?

Ms. OYAMA. We will immediately, if we are notified by a rightsholder, we would remove the link from our search results to The Pirate Bay. We have done that over 5 million times this year. When it comes to copyright——

Mr. BERMAN. You remove the link to a particular item.

Ms. OYAMA. Right.

Mr. BERMAN. Why do you not refuse to de-index the site in your search results?.

Ms. OYAMA. The procedures that Congress set out under the DMCA ensure that today with websites——

Mr. BERMAN. Would it make sense to have a law that allowed you, if the DMCA does not go far enough, a law that essentially told you that is what you should do in response to dealing with a clearly established rogue website that flaunts it in every possible way?

Ms. OYAMA. So, we have no idea of knowing if a given search result is infringing or is authorized. We do need the cooperation of the rightsholder to let us know. And today we are removing links. We think in terms of a legislative approach something that goes after the real incentive for those sites to be in business makes sense. So enhancing the DMCA and going after advertising, which is our services, and payment providers, we think makes sense. We think it is that——

Mr. BERMAN. Could you draft some proposals that reflect that position, so we could look at them? I mean, I would love it if you and the Consumer Electronics Association, and Public Knowledge, and these groups would give us something specific. You think it goes too far, it is too excessive. Give us something specific. Infuse herself with the notion that you want to stop digital theft. What works? And use your brilliant mind that you have into organiza-

tions to give us some specifics, because the DMCA is not doing the job. That is so obvious.

Ms. OYAMA. We are very interested in working with your staff, with the Chairman, and other Members of the Committee. I do believe through NetCoalition, we have provided that language, and would be happy to follow up.

We do think, in terms of search results, that Congress got it right under the DMCA. It leaves up legitimate content. It takes down infringing content. We want to make sure that when we are dealing with speech, that we use a scalpel.

Mr. BERMAN. Well, my time has expired, but you cannot look at what is going on since the passage of the DMCA and say Congress got it just right. Maintain the status quo.

Ms. OYAMA. We certainly believe more tools would be useful.

Mr. SMITH. The gentleman's time has expired. Thank you, Mr. Berman.

The gentleman from North Carolina, Mr. Coble, is recognized?

Mr. COBLE. Thank you, Mr. Chairman. Good to have you. I have had to miss some of the hearing, Mr. Chairman, because of other meetings, but it is good to be here. I was going to examine Ms. Pallante, but the Chairman beat me to it. I was going to examine Ms. Oyama, but Mr. Berman beat me to it. But I will still try to recover.

Ms. Oyama, let me ask you this. What relief does the DMCA offer to a trademark owner who is trying to prevent counterfeiters from selling fakes?

Ms. OYAMA. So, for counterfeit, it is dealt with a little bit differently. For counterfeit at Google, we will act through our advertising. We had eject it, so, for example, for ad words, we have ejected over 100,000 accounts in the last year. There is a very kind of stark difference between copyright and trademark. Congress so far has not enacted by DMCA for trademark. Copyright laws are exclusive rights. Trademarks—it depends on what geography you are in, right, what product you can use. There is a given name specifically that can be used on lots of different products. And so, I know there has been kind of a long-standing conversation about that issue.

Certainly, if we ever were to receive a court order about counterfeit and related to search, well, well of course, we would comply with that court order.

Mr. COBLE. I thank you.

Mr. Clark, how involved are our organized criminal networks in the manufacture and distribution of counterfeit medicines?

Mr. CLARK. From my estimation and experience, it is a problem that is growing. I do not think we have reached the level yet where we are seeing global cartels, per se, as we do in narcotics, but as the notoriety of the crime gets around, the profit margins are so phenomenal and the abilities on a global scale are so low, that it is a no-brainer for organized crime to look at this as a way to go. So, it is growing.

We have seen instances of it, not systemic instances, but we have seen, as I just cited, the Detroit instance, where money was going to Hezbollah. We have seen drug traffickers. But I think it is growing in that capacity.

Mr. COBLE. Mr. Clark, what aspects of SOPA do you believe are particularly important to combating the problem of counterfeiting medicines?

Mr. CLARK. I apologize, Congressman. I missed the first part of that?

Mr. COBLE. What aspects of SOPA, the bill before us, do you believe are particularly important to combating the problem of counterfeiting medicines?

Mr. CLARK. I think all aspects. My biggest worry, Congressman, is that counterfeit medicines are still not perceived by the public, by law enforcement, by judiciary, our judges, and prosecutors as a serious crime yet. When you see somebody like Kevin Xu, who has a global reputation for supplying counterfeits—it was my understanding during his undercover discussions, he offered a list of counterfeit medicines, and he said if anything is on that list, anything else off that list that you want, I can have it for you. Give me 2 weeks. We are talking cancer medicines. We are talking blood pressure medicines. We are talking Alzheimer's medicines.

And I think when we see a few tablets here or there, we have a tendency not to think of the consequences those tablets bring. A lot of people in the United States, I think, look at it and say, there are no bodies in the street. Nobody seems to be dying from counterfeits, so it cannot be that serious of a crime.

Mr. COBLE. I got you.

Mr. CLARK. But when you look at people, at best. If they are getting 20 percent of the active pharmaceutical ingredient in the medicine that they are taking, such as this Alzheimer's medicine that was manufactured in Turkey, manufactured in facilities such as this where there are no conditions that in terms of licensing. Regulatory, environmental, are applied. Even with just 20 percent of the active ingredient in it, what is the other 80 percent? And if there is nothing but benign chemicals in that 80 percent, they are still not going to get relieved of their disease, and they eventually die.

So, my biggest worry, Congressman, people are dying from these counterfeits. We just have not figured out a way to correlate the deaths from counterfeits with the problem yet.

Mr. COBLE. I thank you. I want to beat that red light that will illuminate imminently, and say to Ms. Kirkpatrick, I am advised that MasterCard has been instrumental in combating piracy. And, Mr. Chairman, I think it should be noted, for those of you who have combated, particularly flagrant, that that should be noted. And I thank you all for being with us.

And I yield back, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Coble.

The gentleman from North Carolina, Mr. Watt, is recognized?

Mr. WATT. Thank you, Mr. Chairman. And let me start by thanking all of the witnesses for being here today. This is a difficult issue. This legislation rages some interesting new challenges, but circumstances are raising difficult new challenges.

Ms. Oyama, let me start with you because I want to be sure I understood your testimony. I got the impression that you do not object strenuously to the provisions of Section 102, because they require a court order; that your primary objections are with respect to the provision in 103, where market based system to protect cus-

tomers are involved because it does not require giving notice to the site owner or whoever has put up the site. Am I misstating where you are on that?

Ms. OYAMA. We would certainly agree that concerns about 103 are the greatest, one, because of the scope of what is the definition——

Mr. WATT. Well, let me separate the question. Do you have concerns with Section 102?

Ms. OYAMA. The legislation. We support——

Mr. WATT. The question is, do you have concerns with section 102?

Ms. OYAMA. With some of the remedies, yes.

Mr. WATT. Some of the remedies? Okay. And you will give us that in writing so that we can evaluate those concerns.

Ms. OYAMA. The ads——

Mr. WATT. But your primary concerns are with section 103. Am I misstating that?

Ms. OYAMA. I think the remedies in 102 focused on ads and payments, the way that these sites are making money——

Mr. WATT. I am not trying to get you to resolve that issue about 102 today. I would rather have that in writing.

Ms. OYAMA. It is much more workable, yes.

Mr. WATT. Right. But your concerns about 103 have to do with the lack of notice to the site owner, right?

Ms. OYAMA. It has, in part. I think——

Mr. WATT. Okay. So, is there some effective way that we could give notice to the site owner, that you are aware of? And if you could give me those suggestions in writing, because I have those concerns, too. The problem is we do not currently have an effective way, access to those information to give them notice. And you do, I think, in your system because you put up the site. Okay.

Now, if you could help me with those two things, we will be far down the road. I am not adverse to addressing your concerns. I have indicated that to you both in private and I am saying it publicly today.

Let me talk about this constitutional standard, and make sure that I understand where you are on that because you appear to be advocating a constitutional standard that would prohibit the enforcement of any laws online. In your written testimony, you disagree with Professor Abrams' conclusion that it is constitutional to block access to a website that is primarily infringing, even though such blocking may incidentally impact protected speech.

Your written testimony will not concede that blocking a website that is almost entirely infringing would be constitutional. And you have confirmed that in what you just said verbally here. Does that mean that you consider it unconstitutional for law enforcement to seize a child pornography site if the site also contains one copy of the King James Bible?

Ms. OYAMA. So, the speech concerns that have been raised——

Mr. WATT. Just answer that question for me, and then I will go forward from there.

Ms. OYAMA. There are certainly legitimate problems——

Mr. WATT. What about if it contains 20 copies of the King James Bible, but it is still 90 percent child pornography? Are you saying First Amendment rights will not allow us to do that?

Ms. OYAMA. I think we agree with Floyd Abrams that you need to look at the whole site. You need to make sure that it is really dedicated to infringement—and we need legitimacy.

Mr. WATT. Okay. Well, and probable cause would require the Attorney General's office to do that. I mean, he is not going to go and cite you unless or stop this process unless he has gone through that analysis.

The question is, do you think that there is something unconstitutional about taking down a site that is overwhelmingly, primarily devoted to two stolen products? And I've, you know, if that is your position, I think we are going to have a real problem with that.

Ms. OYAMA. No. I think if there was a site out there that was 100 percent terrible, that is a separate issue. The definition——

Mr. WATT. No, I am saying 90 percent terrible. It's him, saying 98 percent terrible. Is 2 percent going to save the site from being taken down?

Ms. OYAMA. I do not think there is an exact number. I think when you are sweeping in mast majorities of legitimate speech without notice, that raises significant questions——

Mr. WATT. Is that 51 percent, or is it 60 percent? I mean, how are we going to do this? You are telling me I cannot violate somebody's constitutional rights if it incidentally adversely impacts their protected rights. That is what you are saying.

Ms. OYAMA. No. I think if a site was primarily dedicated to infringement, there is a lot of tools that——

Mr. WATT. Okay. Well, that is what the bill says, does it not?

Ms. OYAMA. Well, we would not agree that the scope of the definition captures totally infringing sites. We have a lot of concerns that it sweeps in legitimate——

Mr. WATT. No, I did not say totally infringing. That is not what you said either. That is not what you said. You said primarily infringing. And then, all of a sudden you shifted over to totally infringing. Is this a question about whether something is totally infringing or primarily infringing, or do you think that both of them, that one should be protected and one should not be protected?

Ms. OYAMA. I think a definition that was, you know, narrowly drawn that had something like primarily would be helpful.

Mr. WATT. Okay. So you are going to give us some language on that. My time is up.

Ms. OYAMA. We have a definition.

Mr. SMITH. The gentleman's time has expired. Thank you, Mr. Watt.

The gentleman from Virginia, Mr. Goodlatte, is recognized?

Mr. GOODLATTE. Thank you, Mr. Chairman.

Ms. Oyama, I want to pursue that line of questioning. Years ago, a former Chairman, Henry Hyde, put me in a room with about 30 government representatives from the content industry, from the online industry, Internet service providers, and a few that had a foot in both camps. And we worked for months in a hot room, and came to agreement on the Digital Millennium Copyright Act, and, in particular, the notice and takedown provisions, which you have spoken

highly of. And I agree with you that those provisions still have a role in protecting online copyright.

But the Internet has changed dramatically since then. The speeds have accelerated. The technology is more sophisticated. Search engines are more sophisticated. And the criminals who use all of that to rip off legitimate businesses of all kinds are more sophisticated.

So, as you know, and, as I have said, I am interested in making sure this legislation gives effective tools to combat lawbreakers, but to also ensure it does not entangle legitimate online businesses or the ability of entrepreneurs to continue to bring exciting new products and services to the Internet.

Can you tell the Committee the top concerns the tech community has about the bill and your specific recommendations on how to fix those concerns within the bill?

Ms. OYAMA. Sure, thank you. I think when the conversation started, the idea was to target foreign rogue sites, sites that were clearly breaking the law, build on the DMCA, and introduce new harsh remedies. That is definitely an approach that we would get behind, that we would support. I think when the tech community now is looking at is this language. There are serious concerns that the definition of a site that is dedicated to the theft of U.S. property, you know, probably purely unintentionally, it sweeps in a great amount of lawful websites, so, for example, the unit of analysis for what the site is. There is some language in there that says an Internet site or a portion thereof. So there is some concern about whether we are looking at the whole site or are we just looking at one blog, one tweet, one comment, one page on a site. So, getting the definition right would be really important.

There are other words within the definition that seem to introduce notions like "facilitate." That is one of the reasons why the Consumer Electronics Association, who I mentioned, they have serious concerns because they manufacture so many different devices. Somebody could say that the Internet itself facilitates infringement. So, we need to make sure that we are really staying within the existing confines of copyright law.

I would also mention in the definition there is some language, you can be dedicated to fast if you have. No one understands, sir, what this means. If you have taken deliberate actions to avoid confirming a high probability of the use of your site for infringement.

Right now, small business owners, when they are starting a website, they know if they comply with the DMCA, that they are lawful companies. They can seek investment, they can go forward. If they have to somehow subscribe to that kind of definition, the folks that we are hearing from, they just have no idea how they would even possibly build their sites to build to fit that definition. So I think getting the scope of what is a site dedicated to infringement would be critical.

And from there, we are certainly more than happy to work on remedies. The two that we think are really smart, if you look at Wikileaks, I think this is a good example of the fact that this is a strong remedy, is choking these sites off at their revenue source. They are in business because they can either sell advertising or because they can profit from subscribers. If you could get the entire

industry together and you could choke off advertising, and you could choke off payments to those sites, you would be incredibly effective without introducing the collateral damage that we had discussed to free speech or to Internet architecture, things like that.

So, ensuring that we had the right remedies and the right scope, I think there is plenty of opportunity for all players out for a cross-section of industry to come together.

Mr. GOODLATTE. Let me just follow up on that. The more detailed information you give us, the better our ability to address legitimate concerns. So, will you commit to working with me to identify the specific problems that the tech community has with the bill, and working to address those specific problems to improve the bill as we move forward?

Ms. OYAMA. Absolutely.

Mr. GOODLATTE. And some of have argued that this legislation would break the Internet. As the co-chair of the Congressional Internet Caucus, that is the last thing I want to do. Can you explain exactly how this legislation would impact the functioning of the Internet?

Ms. OYAMA. So, I think the major concerns that have been raised really kind of in a cybersecurity field. So, so there is a white paper by a group of engineers who designed DNS-SEC. There are some other leading cyber security folks who have spoken out about it. I think Stewart Baker has been on record. He is a former Senior Official at DHS, and the formal General Counsel of the NSA.

One of the provisions in the bill would require ISPs to perform DNS blocking. There is kind of a twofold concern there. One is that the methods proposed here are not compatible with a more than 10-year long effort into cybersecurity field to implement DNS-SEC in a way that would prevent cyber security attacks. So, I am not the cyber security expert, but the folks that wrote that code are saying that this will really harm the U.S. in the global effort to make deacons as more secure.

I think the second piece is, we know that users unfortunately, are seeking this material. We can predict that there are going to be circumvention efforts. And so, there is a big concern that if we play certain obligations on you as DNS providers, that users are going to reroute their traffic to offshore rogue providers. And the vulnerabilities that an offshore rogue provider could introduce into the network, not just for the kids that are looking for the movie, or for some bad actor, but for anyone who is on the network that they are on is really significant. It could introduce spyware, malware, privacy concerns.

Mr. SMITH. The gentleman's——

Ms. OYAMA. I know this is, you know, something that really the folks who are the experts in this field have raised, but, you know, that has been kind of a critical concern about——

Mr. GOODLATTE. Ms. Oyama, I hate to interrupt. I do believe that Mr. Clark, if the Chairman will permit Mr. Clark from his past experience with the Department of Justice might also be able to comment on this issue, if the Chairman allows.

Mr. SMITH. Mr. Clark, could you give a very brief response?

Mr. CLARK. Very briefly, unfortunately I do not have the cyber experience. It was not one of the areas I actually worked myself.

I have managed it. I do not know the intricacies about it. So in all honesty, so I apologize for not having an answer for that.

Mr. GOODLATTE. I apologize, Mr. Chairman. I thought there was an opportunity there, but perhaps not. Ms. Oyama, thank you. We look forward to working with you.

Mr. SMITH. Thank you, Mr. Goodlatte.

The gentlewoman from California, Ms. Lofgren, is recognized?

Ms. LOFGREN. Before my questions, I would like to ask unanimous consent to introduce a number of items into the record, opposition to the provisions of the bill. The letters are from the Consumer Union and other consumer groups; TechNet; Tech America; the American Library Association; the Competitive Enterprise Institute; Human Rights Watch and other public interest groups; dozens of human rights groups around the world; a written statement from the ACLU; a paper from the Brookings Institute explaining how the bill would undermine security and stability of the Internet; a white paper by five leading DNS engineers and Internet security experts, a letter from the Anti-Phishing Working Group; an article from Stewart Baker, the former General Counsel of the NSA and Policy Chief for DHS under the Bush Administration entitled "Copyright Bills Could Kill Hopes for Securenet;" a letter signed by AOL, eBay, Facebook, Twitter, Yahoo, LinkedIn, Google, Mozilla, and Zynga; and a Harvard Business Review article entitled "Great Firewall of America."

Mr. SMITH. Without objection.

[The information referred to follows:]

November 15, 2011

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

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

The Honorable Bob Goodlatte
Chairman
Subcommittee on Intellectual Property,
Competition, and the Internet
Committee on the Judiciary
House of Representatives
Washington, DC 20515

The Honorable Mel Watt
Ranking Member
Subcommittee on Intellectual Property,
Competition, and the Internet
Committee on the Judiciary
House of Representatives
Washington, DC 20515

Dear Chairman Smith and Representatives Conyers, Goodlatte, and Watt:

We write to express our concerns with H.R. 3261, the Stop Online Piracy Act. As consumer groups, we agree that consumers should not be harmed by substandard or counterfeit goods. However, we are concerned that some of the measures proposed by this bill and the breadth of its scope could make it more likely to harm consumers' interests. In particular, we are worried the bill could close off online exchanges that provide lower prices for consumers; reduce online security; and allow for anti-consumer practices by online service providers.

Consumer access to online exchanges

Consumers benefit greatly from being able to use the Internet to connect with a wide variety of buyers, sellers, and with each other. Online forums and marketplaces allow consumers to exchange information about products and exchange products themselves in thriving secondary markets. However, the broad language of the bill threatens these activities.

The bill would allow rights holders to send notices to payment processors and advertising networks, ordering them to cut off funding to sites the rights holders believe are "dedicated to the theft of U.S. property." However, this definition is extremely broad. Section 103(a)(1)(B)(ii) defines a "site dedicated to the theft of U.S. property" as including any site whose owner "takes active steps to avoid confirming a high probability" that it is being used (even by others) for infringement. This means that an entirely legitimate site can be defunded, and even enjoined entirely, merely because a few of its users may have infringed. Consequently, overzealous rights holders could shut down lawful exchange sites like craigslist, eBay, swap.com, or BookCrossing, closing off valuable outlets for small-scale buying and selling. For instance, a legitimate student-to-student textbook exchange site could be hampered or shut down by a publisher for the actions of just a few infringing users, raising the costs of an already-expensive education.

Online Security

Secure online communication and commerce is also of critical importance to consumers. Yet, the bill could undermine the security of consumers. Section 102(c)(2)(A) allows for court orders that would block domain name system (DNS) operators from providing access to the Internet Protocol (IP) addresses of targeted sites. In other words, a consumer attempting to access an allegedly infringing site would get an error message or be redirected to another page. However, redirecting DNS queries (to phishing sites and other fraudulent websites) is also a common tactic used by malicious hackers to steal millions of dollars from consumers.

To prevent these tactics, DNSSEC, an important voluntary security standard, is being implemented to ensure that any given DNS query will only return the correct, IP address. However, DNSSEC cannot tell the difference between DNS errors caused by these tactics or by court orders. This means that an ISP cannot simultaneously implement the consumer protections of end-to-end DNSSEC and obey court orders issued under SOPA. ISPs faced with this dilemma may well choose not to implement DNSSEC fully, leaving consumers more vulnerable online.

Furthermore, even under the bill's provision, users could still get to allegedly infringing sites. The simple steps infringers can take to do this, like downloading certain browser plugins or using questionable alternate DNS servers, exposes not only them, but all other consumers, to harm. These considerations mean that DNS blocking is not only largely ineffective, but risks seriously harming consumers' security.

Anti-consumer actions by online service providers

Finally, the bill grants complete immunity to a very large class of actors, including Internet service providers, advertising networks, advertisers, search engines, and payment networks, for cutting off access to a targeted site as long as they can claim their actions were taken in the reasonable belief that the site was suspected of encouraging infringement. This blanket immunity from all federal and state laws and regulations could allow the above actors to act in ways that would harm consumers. For example, Internet service providers could block access to online services that compete with their own telephone or video offerings under a justification of curbing alleged infringement, depriving consumers of legitimate alternatives to high-priced services. The broad immunity of the statute would prevent consumers or consumer protection agencies from policing or addressing such anti-consumer or anticompetitive.

As drafted, the Stop Online Piracy Act has the potential to do more harm to consumers than good. We urge you to reconsider these provisions as you continue to work on the important issue of protecting consumers online.

Respectfully submitted,

Consumer Federation of America
Consumers Union
U.S. PIRG: The Federation of State PIRGs

805 15th St. NW, Suite 708 | Washington, DC 20005
tel. 202.650.5108 | www.technet.org

November 15, 2011

Chairman Lamar Smith
House Committee on Judiciary
2426 Rayburn House Office Building
Washington DC 20515

Ranking Member John Conyers
House Committee on Judiciary
2426 Rayburn House Office Building
Washington DC 20515

Dear Chairman Smith and Ranking Member Conyers:

Thank you for your continued leadership on issues affecting the innovation economy. Your commitment to promoting a strong American economy is greatly appreciated, and TechNet, the policy and political network of CEOs that promotes the growth of technology and the innovation economy, is eager to help you achieve these important goals.

We are writing to express our views about H.R. 3261, the "Stop Online Piracy Act" or SOPA. As an association whose companies collectively touch nearly the entire broadband ecosystem, TechNet is sensitive to the need to stop piracy of online content. The robust flow of digital content for lawful uses is at the core of what makes the internet so important to our economy and society. When the creators of this content are not compensated because their work is stolen, this undermines key features of the internet – the rich store of digital products and commercially relevant information that creates value for consumers and jobs for innovators.

Although H.R. 3261 takes aim at the problem of online piracy, its regulatory approach does so in such a way that could threaten many features that make the internet function well and which allow users to access, create, share, and pay for online content. We have a range of concerns about how SOPA's approach may impact the internet. For example, it may undermine the security of the internet by imposing heavy-handed technology mandates that are also likely to undermine innovation. Additionally, SOPA would inhibit businesses that rely on and facilitate online advertising, as well as those which process payments in electronic commerce.

More specifically, we have concerns about the following provisions:

- The proposal creates a new "private right of action" against lawful U.S. companies. SOPA allows copyright and trademark owners to take action against law-abiding payment processors and advertising companies to compel them to take action against activity on the basis of bare allegations.

- SOPA may subject U.S. internet companies and financial firms to technology mandates, as courts may require companies to take certain actions based on lawsuits brought about by the new private right of action.

- The proposal exposes lawful U.S. firms to significant commercial harm without due process, as firms may have strong incentives under SOPA to stop doing business with sites that are targeted by unproven allegations before due process has played out to prove infringing activity.

- The proposed legislation creates new statutory standards of infringement, which could expose existing and start-up firms in areas such as social media and cloud computing to new litigation and liabilities.

- SOPA undermines efforts to keep cyberspace secure by requiring technological approaches to block access to sites engaging in unlawful acts that facilitate piracy. Illegal sites registered in the U.S. would be blocked under SOPA, but this would encourage such sites to locate overseas – where our nation's recent efforts to improve web security do not apply. The end result is a proliferation of less secure websites registered abroad – sites that facilitate piracy out of reach of U.S. law enforcement.

SOPA also strikes at the heart of the Digital Millennium Copyright Act (DMCA), a 1998 law that established a structure for the enforcement of copyright on the Internet, while establishing a "safe harbor" from infringement liability for internet service providers that act in accordance with the Act's requirements, including through a "notice and take down" process for removing content that infringes copyright.

TechNet members remain committed to fighting online piracy. We feel that the DMCA has established a solid framework for that and additional measures to address the problem should not undermine that valuable foundation. We are concerned that the framework proposed by SOPA threatens to inhibit innovation in the broadband ecosystem, impose burdensome regulatory requirements on the tech sector, while not effectively tackling the problem of online piracy. We look forward to future dialogue with you on this issue.

Best Regards,

Rey Ramsey

President and CEO

TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

November 15, 2011

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

The Honorable John Conyers
House of Representatives
Ranking Member, Judiciary Committee
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers,

On behalf of TechAmerica, the U.S. technology industry's largest advocacy organization representing over 1,000 leading innovative companies, I am writing to express our concerns specifically about the Stop Online Piracy Act (SOPA), but also more generally about the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act).

Fifteen years ago Congress began what would be a lengthy but critically important process of updating copyright law for the new millennium. The end result of that effort was the Digital Millennium Copyright Act (DMCA), which was ultimately informed by hundreds of stakeholders from the newly emerging Internet industry, to Internet service providers, to music and movie companies, to libraries, to civil libertarians, and many more. TechAmerica played a proud and prominent role.

The goals then, as they should be now, were to carefully balance the rights of property holders with the operational realities of "mere conduits," and to directly reach those who infringe or steal other's property. In other words, the goal was to make the rules of the road clear for those who own intellectual property and those who operate service providers or otherwise provide services that may interact with protected intellectual property online – to provide a measured and appropriate approach to intermediary liability.

TechAmerica and our member companies have been quite disturbed by the rise of rogue websites operating offshore, such as The Pirate Bay. These websites detract from the significant technological and commercial innovation ongoing today to help consumers enjoy legally-obtained content on whatever device and in whatever location they want to consume that content. Tools should indeed be provided to challenge the proliferation of such sites that exist to infringe content or to peddle counterfeit goods often to the direct detriment of U.S. companies and our economy. In an attempt to provide such legal tools, both the U.S. Senate and House of Representatives have produced relevant legislation.

Protecting intellectual property must be a cornerstone of U.S. policy as both global trade and e-commerce grow. TechAmerica members are among the most innovative companies in the United States, producing cutting edge electronic components, consumer electronics and industrial systems, jet engines and educational software, for example. The increasing use of e-commerce,

or sale of products over the Internet, has allowed the proliferation of "rogue" websites, sites that are set up outside of the United States to sell counterfeit products that violate the trademarked brands of their rightful owners, and deceive buyers as to the quality and origin of the goods. These counterfeit products are making their way into the supply chain at a loss to the IP owner, but also at a risk to the end user of a wide range of consumer, industrial and defense related products. These rogue sites are exploitive and dangerous to the public and U.S. competitiveness, and policy makers should seek to shut them down.

Sadly, neither chamber of Congress has produced thoroughly acceptable legislation, but SOPA in particular marks a clear retreat from a history of Congressional support of the digital revolution. That support has often come in the form of not imposing regulation on the industry, and certainly never before has such a wholesale shifting of costs and responsibilities of property owners onto technology companies been contemplated -- a shift away from a careful balance and toward legislation that favors one industry over another.

Put another way, the approach taken in SOPA leads one to wonder why the DMCA would even be used in the future. Using SOPA's proposed broad new inducement provision, one could simply ignore the current DMCA safe harbors and use intermediaries to accomplish the end goal, and if damages were warranted, merely later sue for infringement. Moreover, important measures to make sure that the proposals keep pace with technology, such as the DMCA requires with the triennial rulemaking on exceptions to the prohibition on circumvention of access and use controls, are non-existent. Along those same lines we are also dismayed that the proposed legislation relies on "simple" technical measures to address complex international issues that are likely better handled through diplomacy, negotiation, constructive dialog and coordinated action. The proposed "solutions" carry risk, perhaps significant, and are likely to be easily circumvented.

That said, while the DMCA provides a relevant and informative model, it does not cover key challenges such as counterfeiters selling their physical products on the Internet. The potential damage that counterfeit products bring to a company's or industry's reputation and to the integrity of systems dependent on those products is serious and does deserve attention.

Massive cost shift

SOPA merely shifts costs from content owners, the rightful protector of their content, to various other parties, rather than making sure that costs are appropriately placed.

This is a philosophical issue that runs to the heart of both proposals. Do we really want government forcing one industry to subsidize another, to be required by force of law to assist another industry in being successful? More typically we expect industries to operate within a market framework and with the freedom of contract to solve such challenges. In this case, Congress seems determined to step in and force one industry to provide subsistence to another. However, as evidenced by the measured Memorandum of Understanding reached between the content industry and ISPs earlier this year, interested parties can and will work together to combat intellectual property infringement in lieu of government intervention.

So what are the costs? Simply put, they are the costs of stopping bad guys from doing bad things to other people's property – the cost of compliance, liability and distraction from improvement from the products of the technology industry.

Safe Harbor No More

One key factor that allows the economics of many legislative models to work is the inclusion of a clear and dependable safe harbor. This inclusion should make clear to intermediaries that if they are engaged in any wrong doing then they will find no solace in the law, but if intermediaries are acting in good faith then they could step out of the way of the costs and allow the rights holder to bring their claim directly against the alleged infringer.

Under SOPA, a "service provider" will be required by a court order to take, at the instruction of the Attorney General, "technically feasible and reasonable measures...including" DNS redirects. What are those limits? Are there any? And to the extent there may be some, then how many court cases will it take to discover them?

Expansive Definitions

In general, the definitions are sweeping and unclear in nature, sweeping in more than less. For example, in SOPA the definition of "service provider" includes both ISPs and online service providers, which means it could include anyone with a website. In other places, definitions of "ad networks" and "payment processor" are not well defined.

Another example is the definition of a dedicated infringer or sites that were claimed to be "dedicated to the theft of U.S. property." Again, while the thought is right, the definition is sweeping. No one supports those who would steal or attack the very heart of U.S. innovation, but the definition is so broad, going beyond sites that are primarily designed or are marketed for infringing purposes, that many cloud-based services could be implicated even when they would not be recognized as a dedicated infringer under any reasonable definition. The new proposed language also includes sites whose operators "avoid confirming a high probability" that they will be used to infringe or who had at any previous time promoted infringements.

The context set out in the proposals is equally broad as it focuses on "sites" that can be one page of a broader, as they are colloquially known, website. Hundreds, thousands, and even millions of Web "sites," as contemplated in SOPA, make up what might more aptly be called a domain.

Likewise, the proposal to impose felony criminal charges for the illegal streaming of copyrighted works potentially captures a number of parties who offer services or products that primarily are intended to allow consumers to consume legally-obtained content in a variety of different settings. The "rule of construction" proposed in SOPA attempts to rectify this problem, but appears to focus on contract disputes between video distributors and content producers. Unless this carve out is expanded to include companies making a good faith effort to innovate and develop new products and services that give consumers a means to consume content they have obtained legally, Congress runs the risk of hampering innovation, investment, and job creation in this incredibly dynamic space.

Due Process Ignored
One of the more egregious aspects of SOPA is the overbroad standard for secondary liability, the end result of which treats sites as guilty until proven innocent. Under this proposed law, no court would be involved in the process until and unless a site operator filed counter-notice asserting that the site did not fit the broad definition of dedicated infringer. One is hard pressed to think of another place where lawmakers would be comfortable designing a system that allows a mere accusation without any court review to lead to potentially damaging actions against another. Courts do serve a role in our legal system, as a neutral arbiter to balance concerns, rights and responsibilities of several interests.

In this case, one obviously biased party can cause harm without any such review. Network advertisers (which are now largely technology-based and technology-driven companies), credit card companies and other payment processors such as PayPal would be required to stop providing ads or payment services to any site that a copyright or trademark holder claimed was "dedicated to the theft of U.S. property." Again, all without court review. The damage to the business of the wrongly accused would be stifling.

Private Right of Action Difficulty
The PROTECT IP Act also raises concerns regarding the authority vested in rights holders to bring injunctions against sites they accuse of participating in infringing activities. But worse, the private right of action provisions in SOPA go well beyond those in the Senate bill.

As mentioned above, the private right of action is particularly troubling because of the ability of an accuser to wreak havoc outside of the court system. Some will argue that the newly created DMCA-style notice-and-takedown process for ad networks and payment processors is a system that can work; however, the proposed system stands the original notice-and-takedown system on its head by changing up the reason for its being. In the DMCA such a system was designed at the request of all parties to lower costs by moving away from a cease and desist letter tradition. Generating a notice has proved less expensive and removes the intermediary from the conversation, allowing the rights holder to directly engage with the accused wrong doer. Here the system is designed to place intermediaries squarely in the middle of the action, leaving intermediaries holding the cost, liability and compliance bag.

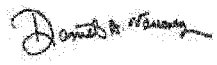
Extra-territorial Problems
The extra-territorial reach of the bill is problematic both for U.S. foreign policy and for those engaged in Internet Governance in the international arena. One of the significant issues is the balkanization of the Internet; an unhealthy fragmentation that could result from blunt technological implementation of well-intentioned policy imperatives. To date, the U.S. has largely avoided extra-territorial reach, and consequently the U.S. can speak authoritatively and forcefully against any such measures. Enacting SOPA or even the Protect IP Act will signal that the United States not only supports these measures, but more importantly, supports imposing restrictions through technical means at the most basic levels of the Internet.

Technology and Security Concerns
While we have many remaining concerns, we are compelled to address the proposal's quick assertion of specific technological fixes. For example, the requirement that ISPs block their customers from reaching an accused infringer site (i.e. DNS filtering), particularly in the voluntary immunity provisions that contain no court review, causes concern. Notably, this approach would undermine important security measures and be technically infeasible with DNS Security Extensions (DNSSEC), which allows secure authentication of Internet assets, is critical for combating the distribution of malware and other problematic behavior, and has high-level US Government support and investment. Further, such filtering requirements would encourage consumers to use alternate servers, which would promote the development of techniques and software that circumvent the use of the DNS and, therefore, undermine the value, security, and resiliency of a single, unified, global communications network.

In the end there is great support for stopping bad actors. The question is how they might be effectively stopped without burdening one industry with the costs more correctly borne by the rights holders. TechAmerica would very happily bring to bear its historical and current intermediary liability expertise in assisting both the House and Senate in moving forward to meet the goals of providing needed tools to stop bad actors, while finding a way to avoid forcing the technology industry into an untenable economic situation.

Only carefully crafted solutions that seek to correctly assign burdens based on who most correctly should bear them, like the owners of property, and that protect the innocent while allowing for pursuit of malcontents will allow the Internet to flourish full of robust content well protected and appropriately used. Unfortunately, SOPA does not meet this threshold and hence TechAmerica cannot support this bill as introduced, but stands ready and willing to work with both chambers of Congress to improve the legislation.

Sincerely,



Dan Varroney
Acting President and CEO
TechAmerica

cc: Members of Congress

November 8, 2011

Chairman Lamar Smith
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member John Conyers
House Committee on the Judiciary
B-351 Rayburn House Office Building
Washington, D.C. 20515

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

Dear Chairman Smith and Ranking Member Conyers:

I write on behalf the Library Copyright Alliance (LCA), consisting of three major library associations—the American Library Association, the Association of College and Research Libraries, and the Association of Research Libraries—that collectively represent over 139,000 libraries in the United States employing over 350,000 librarians and other personnel. I write to express our serious concerns with the Stop Online Piracy Act (SOPA). While we agree with many of the criticisms raised by others with respect to Title I, this letter will focus on problems section 201 could cause for libraries and their users.

Two provisions of section 201—the definition of willfulness in section 201(c) and the expansion of criminal penalties to public performances in section 201(a)—are troubling. While each provision is problematic in its own right, the two together could threaten important library and educational activities.

I. Definition of Willfulness

Section 201(c) contains a rule of construction concerning the term "willful" that could substantially expand the range of activity considered criminal copyright infringement.

The Copyright Act recognizes three different levels of intent for infringement: innocent infringement, ordinary infringement, and willful infringement. The Copyright Act defines an innocent infringer as an infringer that "was not aware and had no reason to believe that his or her acts constituted an infringement of copyright...." 17 U.S.C. § 504(c)(2). Willful infringement is not defined in the statute, but has been understood by courts to mean a "voluntary, intentional violation of a known legal duty." Regular infringement falls between these two extremes, *e.g.*, when a person believed that his action were noninfringing but this belief was unreasonable. Different statutory damages

attach to these different levels of intent. The range of statutory damages for ordinary infringement is $750 to $30,000 per work infringed. 17 U.S.C. § 504(c)(1). In cases of willful infringement, the court can increase the statutory damages to $150,000; in cases of innocent infringement, the court can reduce the statutory damages to $200.[1]

Additionally, willful infringement is subject to criminal sanctions. This is where section 201(c) of SOPA comes into play. Section 201(c) provides that a person "acting with a good faith reasonable basis in law to believe that that the person's conduct is lawful shall not be considered to have acted willfully" for criminal copyright purposes. This rule of construction creates a negative implication that a person is a willful infringer if the person did not have a good faith reasonable basis in law for believing that his conduct was lawful. Thus, if a court finds that the person's belief was unreasonable, the court might consider him a willful infringer, even if the person in good faith believed his actions were legal. Under current law, however, this level of intent constitutes ordinary infringement, not willful infringement. In other words, the rule of construction could have the effect of collapsing the three levels of intent into two: willful infringement and innocent infringement. The willful infringement level would swallow the ordinary infringement level, thereby significantly broadening the range of activities subject to criminal sanctions.

II. Criminal Sanctions for Public Performances

Section 201 extends criminal sanctions for public performances such as streaming, but does so in a manner far broader than similar legislation in the Senate, S. 978.

Under current law, infringing public performances are subject to lower criminal penalties than infringing reproductions or distributions. A willful infringer of the public performance right can only be subject to misdemeanor (as opposed to felony) sanctions, and only if the infringement was for purposes of commercial advantage or private financial gain. *See* 18 U.S.C. § 2319(b)(3). S. 978 would allow felony penalties for a public performance for commercial advantage or private financial gain. However, S. 978 would leave the status quo of no criminal penalties for public performances without purpose of commercial advantage or private financial gain.

Section 201 of SOPA makes the same amendment as S. 978 for commercial performances. But, SOPA also imposes criminal penalties for public performances by means of digital networks with a retail value of more than $1,000. *See* proposed section 506(a)(1)(B). Felony penalties would be available if the retail value is more than $2,500. *See* section 201(b)(2). Thus, section 201 of SOPA for the first time authorizes both misdemeanor and felony penalties for non-commercial public performances.

[1] When the infringer is a nonprofit educational institution, library, archives, or public broadcasting entity, the court can remit statutory damages altogether.

III. Impact of Amendments on Libraries

There are three pending copyright infringement lawsuits against universities and their libraries relating to their use of digital technology.[2] One of these cases, *AIME v. UCLA*, concerns the streaming of films to students as part of their course assignments. These lawsuits reflect a growing tension between rights holders and libraries, and some rights holders' increasingly belligerent enforcement mentality. Moreover, legislation such as SOPA and the PRO-IP Act passed in the 110th Congress, and the activities of the Intellectual Property Enforcement Coordinator (a position created by the PRO-IP Act), encourage federal prosecutors to enforce copyrights law more aggressively.

In this environment, the criminal prosecution of a library for copyright infringement is no longer beyond the realm of possibility. For this reason, we strongly oppose the amendments described above, which would increase the exposure of libraries to prosecution. The broadening of the definition of willful infringement could result in a criminal prosecution if an Assistant U.S. Attorney believes that a library's assertion of fair use or one of the Copyright Act's other privileges is unreasonable. This risk is compounded with streaming, which SOPA would subject to felony penalties even if conducted without purpose of commercial advantage or private financial gain.

To be sure, section 201(c) states that a person is not acting willfully if he is "engaged in conduct forming the basis of a bona fide commercial dispute over the scope [or] existence of a contract or license governing such conduct...." But this would provide little comfort to libraries in disputes relating to streaming because of the second clause of the sentence: "where such person has a reasonable basis in law to believe that such conduct is noninfringing." So long as the prosecutor believes that the library's interpretation of the license is not reasonable, the existence of the license will not protect the library from the claim that it acted willfully.

Accordingly, the rule of construction in section 201(c) should be amended to eliminate any possible negative implication that broadens the scope of willfulness. Additionally, section 201(a) and (b) should be amended so that they do not apply to streaming and other public performances for non-commercial purposes.
We would be happy to answer any questions you may have. We look forward to working with you and your staff as the legislation moves forward.

Respectfully,

Brandon Butler
ARL Director of Public Policy Initiatives, on behalf of LCA

---

[2] *Cambridge University Press v. Patton* (three publishers sued Georgia State University concerning its electronic reserve system); *Association for Information Media and Eqipment v. Regents of the University of California* (film distributor sued UCLA concerning its streaming of films to students); and *Authors Guild v. HathiTrust* (authors associations sued a consortium of libraries concerning the assembly and use of a digital repository of books).

Competitive Enterprise Institute
Free Markets and Limited Government

Published on *Competitive Enterprise Institute* (http://cei.org)

Congress Should Amend SOPA to Address Cybersecurity, Due Process Concerns

Congress Should Amend SOPA to Address Cybersecurity, Due Process Concerns

Significant Issues Remain Unresolved After Today's Hearing
By Nicole Ciandella [1]
November 16, 2011

Washington, D.C., November 16, 2011 – This morning, the House Judiciary Committee held a hearing [2] on H.R. 3261, the Stop Online Privacy Act. Below is a statement from **CEI Associate Director of Technology Studies Ryan Radia** [3], who attended the hearing.

Members of the House Judiciary Committee deserve credit for working to tackle the serious problems that rogue websites pose to American consumers, jobs, content creators, and business large and small. But missing from today's hearing was a substantive discussion of SOPA's practical implications for venture capital firms, Internet startups, and cybersecurity.

While new legislation is indeed needed to combat rogue foreign websites that violate U.S. laws flagrantly and with impunity, SOPA's definitions and remedies are too broad and too vague in their current form. They would cast a cloud of legal uncertainty over America's innovative, startup-driven Internet economy.

Legitimate, user-driven websites often contain both lawful and unlawful content. Cutting off their economic lifeblood should be a last resort. It would be a grave mistake to grant enormous discretion to Justice Department and rights holders and assume that they, and inexpert federal trial judges, will interpret SOPA's unclear provisions is construed as narrowly as they must be to protect this economy.

If anything, today's hearing made clear just how much work remains to be done to craft an effective but targeted approach to rogue sites. Serious questions remain unresolved about cybersecurity, due process and free speech. Additional hearings are needed to explore these important issues with Internet engineers, law professors, and venture capitalists.

As the House Judiciary Committee explores revisions to SOPA to address concerns about the bill, members should consider implementing the following ideas:

- Amend Section 102's definition of a foreign infringing site to encompass only sites that are primarily dedicated to infringing activities rather than sites that are used in any part or manner to facilitate infringement;
- To address serious cybersecurity concerns, remove requirements that service providers prevent access to the domain names of sites found to be dedicated to infringement but leave intact remedies involving payment processors and advertising networks;
- Amend Section 103 to require qualifying plaintiffs to bear the costs of injunctions improperly issued under SOPA, regardless of good faith;
- Eliminate the vague prong of the definition of infringing sites at § 103(a)(1)(B)(ii)(I), which includes sites that have taken "deliberate actions to avoid confirming a high probability [of infringement]."
- Exempt from Section 103's extraordinary remedies all U.S.-based, DMCA-compliant websites against which U.S. law enforcement authorities are able to enforce civil and criminal judgments entered by U.S. courts;
- Amend Section 201 to impose felony penalties only on willful infringement committed for commercial advantage or private financial gain;
- Clarify that willful infringement requires an intent to violate a known legal duty for criminal copyright infringement purposes.

Competitive Enterprise Institute | 1899 L ST NW Floor 12, Washington, DC 20036 | Phone: 202-331-1010 | Fax: 202-331-0640

Source URL: http://cei.org/news-releases/congress-should-amend-sopa-address-cybersecurity-due-process-concerns

Links:
[1] http://cei.org/staff/nicole-ciandella
[2] http://judiciary.house.gov/hearings/hear_11162011.html
[3] http://cei.org/expert/ryan-radia

November 15, 2011

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

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

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

Dear Chairman Smith and Ranking Member Conyers,

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

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

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

We also have serious concerns about the inclusion the provisions in section 102 to require ISPs to filter Domain Name System (DNS) requests or otherwise try to "prevent access" to targeted websites.[1] DNS-filtering is trivial to

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

circumvent and will be ineffective at stopping infringement. Where it does have an impact, that effect is likely to be overbroad, sweeping in legitimate online content. We have witnessed this already in the case of mooo.com, the seizure of which led to upwards of 84,000 innocent subdomains being blocked.[2]

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

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

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

Sincerely,

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

---

many of these organizations have also publicly opposed http://www.publicknowledge.org/Public-Interest-Letter-PROTECT-IP-Act.

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

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

November 15, 2011

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

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

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

Dear Chairman Smith and Ranking Member Conyers,

As press freedom and human rights advocates, we write to express our deep concern with H.R. 3261, the Stop Online Piracy Act (SOPA). While this is a domestic bill, there are several provisions within SOPA that would have serious implications for international civil and human rights which raise concerns about how the United States is approaching global internet governance. The United States has long been a strong advocate for the protection and promotion of an open Internet. However, by institutionalizing the use of internet censorship tools to enforce domestic law in the United States creates a paradox that undermines its moral authority to criticize repressive regimes.[1] We urge the United States to uphold its proclaimed responsibility as a leader in internet freedom and reject bills that will censor or fragment the web.

Through SOPA, the United States is attempting to dominate a shared global resource. Building a nationwide firewall and creating barriers for international website and service operators makes a powerful statement that the United States is not interested in participating in a global information infrastructure. Instead, the United States would be creating the very barriers that restrict the free flow of information that it has vigorously challenged abroad. By imposing technical changes to the open internet while eroding due process, SOPA introduces a deeply concerning degree of legal uncertainty into the internet economy, particularly for businesses and users internationally. Business cannot be conducted online when international users and businesses do not have faith that their access to payments, domain names, and advertising will be available, raising challenges to economic development and innovation. **This is as unacceptable to the international community as it would be if a foreign country were to impose similar measures on the United States.**

The provisions in SOPA on DNS filtering in particular will have severe consequences

[1] http://blogs.lse.ac.uk/mediapolicyproject/2011/11/02/freedom-abroad-repression-at-home-the-clinton-now-cameron-paradox/

worldwide. In China, DNS filtering contributes to the Great Firewall that prevents citizens from accessing websites or services that have been censored by the Chinese government.[2] By instituting this practice in the United States, SOPA sends an unequivocal message to other nations that it is acceptable to censor speech on the global Internet. Additionally, Internet engineers have argued in response to the Protect IP Act, DNS filtering would break the internet into separate regional networks.[3] Worse still, the circumvention technology that can be used to access information under repressive Internet regimes would be outlawed under SOPA, the very same technology whose development is funded by the State Department.

SOPA puts the interests of rightsholders ahead of the rights of society. SOPA would require that web services, in order to avoid complaints and lawsuits, take "deliberate actions" to prevent the possibility of infringement from taking place on their site, pressuring private companies to monitor the actions of innocent users. Not only will this effectively negate the safe harbor protection provided in the Digital Millennium Copyright Act (DMCA), but the proposed legislation would disproportionally affect small online communities who lack the capacity to represent their users in legal battles. Wrongly accused websites would suffer immediate losses as payment systems and ad networks would be required to comply with a demand to block or cease doing business with the site pending receipt of a legal counter-notice. Even then, it would still be at the discretion of these entities to reinstate service to the website regardless of the merits of an alleged rightsholder's claim, robbing online companies of a stable business environment and creating a climate where free speech is subject to the whims of private actors.

Censoring the internet is the wrong approach to protecting any sectoral interest in business. By adopting SOPA, the United States would lose its position as a global leader in supporting a free and open Internet for public good.

The international civil and human rights community urges Congress to reject the Stop Online Piracy Act.

Best regards,

Access
AGEIA DENSI (Argentina)
ahumanright.org
Association for Progressive Communications (APC)
Bits of Freedom (The Netherlands)
Center for Media Justice
Center for Rural Strategies
Centre for Internet and Society (India)

---

[2] http://opennet.net/research/profiles/china

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

Church of Sweden
Communication Is Your Right!
Computer Professionals for Social Responsibility
Consumers International
Derechos Digitales (Chile)
Digitale Gesellschaft e.V. (Germany)
Digital Rights Ireland
Electronic Frontier Finland (Effi)
European Digital Rights (EDRi) (Association of 27 digital rights groups from around Europe)
Center for Technology and Society (CTS/FGV) (Brazil)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
(Germany)
Free Network Foundation
Free Press
Free Software Foundation
Global Partners & Associates
GreenNet (England)
The Julia Group (Sweden)
Instituto Nupef (Brazil)
Index on Censorship
Internet Democracy Project (India)
Karisma (Colombia)
La Quadrature du Net (France)
May First/People Link
MobileActive.org
Net Users' Rights Protection Association (NURPA) (Belgium)
Open Rights Group (ORG) (UK)
Open Spectrum Alliance
Palante Technology Cooperative
The Public Sphere Project
Reporters Without Borders / Reporters sans Frontières
Virtual Activism
wlan slovenija (Slovenia)
10com (European Union)

Written Statement of the American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Michael W. Macleod-Ball
Chief of Staff/First Amendment Counsel

Submitted to the House of Representatives
Committee on the Judiciary

November 15, 2011

"Stop Online Piracy Act"

Chairman Smith, Ranking Member Conyers, and Members of the Committee:

We offer this statement for the record in connection with the hearing on H.R. 3261, the "Stop Online Piracy Act" (SOPA). The bill is a well intentioned effort to reduce the infringement of copyrighted material online. We share the sponsors' goal in that regard. As introduced, however, the bill is severely flawed and will result in the takedown of large amounts of non-infringing content from the internet in contravention of the First Amendment of the U. S. Constitution. Accordingly, we urge the Committee to set aside this bill in its entirety or, alternatively, to reformulate the bill so it is narrowly focused on providing an effective and adequate remedy to those content producers whose copyright interests are infringed by the activities of others, without impacting non-infringing content.

The American Civil Liberties Union (ACLU) is a non-partisan advocacy organization having more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide. We are dedicated to the principles of individual rights, equality, and justice as set forth in the U. S. Constitution. For more than 90 years since its founding, the ACLU has been America's leading defender of First Amendment free speech principles. Most relevant to the current hearing, we led the way in landmark federal litigation establishing the principle that online speech deserves the very same protections as offline speech.[1]

By their very nature, laws protecting copyrights constrain free speech and access to information. Unlike other speech restrictions, however, copyright laws may also advance the generation of information and ideas. A robust copyright system encourages free speech by giving speakers incentives to create and disseminate works of authorship. Such laws add to the marketplace of ideas by encouraging the creation of more content through the assurance that content producers will receive the fruits of their labor. But access to information of all kinds – even disfavored information - is a fundamental right that must be protected. Even more to the point, the mere existence of infringing content online does not justify the removal of non-infringing content in the course of attempting to rid the internet of the former. These established principles should not change or be treated differently just because technology has changed.

- **Background**

Copyright protection in theory only impacts the speech rights of those who would steal the rights in works entitled to protection. But the implementation of such a system can have an effect that goes far beyond the copyright pirate and restrict perfectly lawful non-infringing content. Such is our concern with SOPA and such was our concern with two preceding bills in the legislative process. The Senate Judiciary Committee considered S. 3804, the Combating Online Infringement and Counterfeits Act (COICA) near the end of the 111th Congress. Despite significant changes incorporated into the bill, the bill would have impacted online content that had no infringing qualities. Further, the bill was insufficiently narrowly tailored to minimize its impact on such protected content. In the current Congress, S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP)

[1] Reno v. ACLU, 521 U.S. 2329, 2344 (1997).

received approval of the Senate Judiciary Committee but remains stalled short of the Senate floor. PROTECT IP is a significant improvement over COICA in that it uses a narrower definition for the term "dedicated to infringing activity". By narrowing the definition, the drafters thereby limited the number of online sites that would become subject to restrictive court orders. While the new definition did not eliminate impact on non-infringing content and while we were unable to support the bill for that reason, it clearly was an improvement over COICA.

SOPA, unfortunately, is substantially worse than PROTECT IP. By eliminating the concept of sites 'dedicated to infringing activity', SOPA enables law enforcement to target all sites that contain some infringing content – no matter how trivial – and those who 'facilitate' infringing content. The potential for impact on non-infringing content is exponentially greater under SOPA than under other versions of this bill. As such, despite our support for the protection of the legitimate copyright interests of online content producers, we cannot support SOPA, and in fact we oppose it in its current form, given its broad sweep and its heavy hand that will land largely upon innocent content producers. We urge Committee members to focus not just on the goal of protecting copyright owners, but also protecting the speech rights of consumers and providers who are reading and producing wholly non-infringing content and to eliminate the collateral damage to such protected content. Only in that way will the Committee truly achieve its goal of protecting authors and allow the legislation to survive constitutional challenge.

- **SOPA Will Restrict Non-Infringing Online Content**
    - **Attorney General Actions**

Under SOPA, the Attorney General would identify an internet site that is 'committing or facilitating the commission' of an online copyright infringement.[2] Once established, the Attorney General would have authority to serve the court order affirming the infringement upon any internet service provider (ISP), search engine, payment network provider, or internet advertising service. The ISP would be obliged to prevent access by its subscribers to the infringing site. The search engine would be compelled to prevent the infringing site from 'being served as a direct hypertext link'. The payment network provider would have to suspend payment transactions involving the infringing site. The internet advertising service would be barred from providing ads for the infringing site.[3] Such orders might be acceptable if they only affected infringing content. But a site with infringing content almost always has a wealth of non-infringing content as well. By contemplating an order that effectively bars others from gaining access to both infringing and non-infringing content, the proposed statute goes beyond appropriate First Amendment free speech protections.

A speech restriction will fail unless it is designed to achieve a compelling public purpose and does so by being narrowly tailored to achieve its stated purpose.[4] Courts have held a very strict line in determining if a statute's scheme is narrowly tailored – striking down laws banning

---

[2] S. 3261, Section 102 (a)
[3] *Id.* at Section 102 (c).
[4] Sable Comm'ns of Calif. v. FCC, 492 U.S. 115, 126 (1989).

animal crush videos, violent video games, and indecent online material.[5] A court may very well find that stopping online piracy is a legitimate public purpose, perhaps even a compelling one. But the scheme presented in SOPA is far from narrowly targeted at infringing content. Just compare it to the other pending bill – PROTECT IP. That is only one example of how to protect online copyrights with a lesser impact on non-infringing content. While we think even PROTECT IP falls short of adequately protecting non-infringing content from removal, the bill nonetheless serves as Exhibit A in establishing that SOPA falls short of the constitutional requirement. As long as SOPA's statutory scheme seeks to impact sites that are something other than pervasively and grossly infringing, we will continue to have very grave concerns for the statute's constitutionality.

- **Internet Advertising Services**

As a separate matter, the section barring internet advertising services from providing ads relating to the infringing site or from making ads for the infringing site is far too broad. While a payment interdiction order would avoid impact on the First Amendment protection of free speech, an order barring the creation or delivery of ads which may not have anything whatsoever to do with infringing content violates the speech right of the advertising service. The section relating to internet advertising services should be eliminated from the bill or, at the very least, limited in scope to a payment interdiction scheme for those services that are directly tied to infringing content.

- **Market-Based Actions**

SOPA also contains another remedy for those who are the victims of online infringement – one that allows the victim to take action independently. Copyright infringements at their core are private commercial disputes. One person holding a copyright is damaged by another's infringing use of that protected content. The remedy should in most cases be one that compensates the content producer with the profits gained by the infringer or the profits lost due to the infringement. Accordingly, market-based actions make sense – and such a remedial scheme has the advantage of minimizing a direct government role in restricting speech. A real danger of overreach and/or conflict exists if the federal executive branch plays a major role in deciding what content stays up on the internet and what content comes down.

But the market-based system proposed in SOPA is as flawed as the Attorney General system. The sites that a copyright holder can target include sites that often contain non-infringing content in addition to the allegedly infringing content.[6] The SOPA scheme is especially egregious because there is no obligation to seek court approval and the copyright holder has no incentive to narrow the scope of the proposed takedown to minimize impact on non-infringing material. A

---

[5] U.S. v. Stevens, 130 S. Ct. 1577 (2010) (animal cruelty); Brown v. Entertainment Merchants Ass'n, 131 S. Ct. 2729 (2011) (violent video games); Reno v. ACLU, 521 U.S. 2329, 2344 (1997) (Communications Decency Act).

[6] S. 3261 at Section 103 (a). *See also* Kathy Gill, *Congress Bows to Hollywood, Introduces Bill to Fundamentally Alter Internet Infrastructure*, The Moderate Voice (Oct. 27, 1022) (takedown of infringing material will also result in takedown of non-infringing material) *available at* http://themoderatevoice.com/126684/congress-bows-to-hollywood-introduces-bill-to-fundamentally-alter-internet-infrastructure/.

copyright holder may provide a notice to a payment network provider or an internet advertising service, which must then take the same steps it would have to take under the court order described above. While there is no provision in the bill for issuing orders to search engines or ISPs, the authorization of an outright ban of advertising content is of questionable constitutional propriety and the absence of court oversight of such a process makes a flawed system even worse.

- **Other issues**

  - *'Facilitating' the commission of infringement.* SOPA's threshold for action rests on the existence of a site that contains infringing material or 'facilitates' such infringement. Yet the statute fails to define the activities that would comprise 'facilitation'. Could the mere unintentional provision of a link to an infringing site that contains predominantly non-infringing content be construed as 'facilitating' if the target site also has infringing content? Some who support this bill argue that is not the intention. At the very least, the bill should define 'facilitation' so as to incorporate an intent requirement and to ensure that facilitation benefitting a site that is not pervasively infringing does not warrant the harsh remedies set forth in the bill.

  - *Adequate Notice and Opportunity to be Heard.* Service of process provisions for actions under SOPA fail to assure that those having interests in the content to be removed from the Internet have an opportunity to receive notice and an opportunity to be heard before the seizure order is issued. SOPA only requires the government to send a notice of alleged violation and intent to proceed to a domain name's registrant or the owner or operator of the internet site, and only if the email and postal address are available. Such a standard is substantially less than required in most federal proceedings, where the standard calls for personal delivery upon the party or an officially designated agent.[7] Service by publication is authorized in certain limited circumstances, but typically only as a last resort upon showing that a party cannot be served by other means.[8] While most people agree that online infringement continues to impact copyright holders and content producers, no justification exists to sidestep tried and true procedural protections available to all others who are called to account before the federal courts. Especially because of the implications for non-infringing First Amendment protected materials, the Committee must not permit such weakened notice provisions to control. Instead, the Committee should require true advance notice of proceedings before issuance and enforcement of a seizure order. This is especially true since in many case there is a possible financial remedy available through the payment interdiction remedy.

  - *Alternative enforcement and remedies*. A pursuit of the proceeds of infringement poses fewer constitutional risks than the proposed seizure regimen and we urge you to focus and perhaps expand upon that alternative approach. Even if the Committee decides to retain the seizure format, it should encourage alternative enforcement mechanisms. When the non-infringing content that would be taken down is

[7] Fed. R. Civ. Proc. 4.
[8] *See, e.g., id.* at 71A.

substantial in volume, or when there is a real question whether the content provider has received actual notice, deferral to such an alternative remedy seems especially appropriate. First Amendment risks are especially acute when a government actor is in the position of deciding whether to prosecute such cases. When the courts are in the position of properly framing the seizure order that effectively removes content from the internet, the court must minimize or eliminate the impact on non-infringing content. SOPA does not contemplate the issuance of such narrowing court orders, however. Instead, such orders – when the court is involved – merely provide the moving party the authority to demand that third parties cooperate in the process of removing online content. Such a system can only be saved by setting aside the emphasis on taking down content and substituting a system that emphasizes interdicting the flow of money to infringing sites.

- **Setting an Example for the World**

We are concerned with the example that an overly broad online infringement takedown scheme would set for other countries with fewer free speech protections. Even established democracies – Great Britain, France, Germany – have lesser speech protections than the United States. And as events of the ongoing 'Arab Spring' demonstrate, other more totalitarian nations have abused and will continue to abuse their technological capacity to take down content they find objectionable or threatening. Secretary of State Clinton has voiced strong support for international open internet principles and standards, even while affirming that there is no inconsistency between free speech principles and strong online copyright protections.[9] Such considerations make it all that much more important to ensure that any internet content restriction be confined strictly and solely to infringing content so that America can continue to advocate vigorously for truly open Internet standards on the international stage.

[9] Indira A. R. Lakshmanan, *Clinton to Support Facebook Freedom, Fight Censorship*, Bloomberg BusinessWeek (Feb. 16, 2011) *available at* http://www.businessweek.com/news/2011-02-16/clinton-to-support-facebook-freedom-fight-censorship.html; *see also* Letter from Secretary Clinton to Rep. Howard L. Berman (Oct. 25, 2011).

A strong system of copyright protection for online content is critical to the continued success of the flourishing internet marketplace of ideas. But Congress must not provide that protection at the expense of taking down non-infringing content. We urge the Committee to reject SOPA in its present form and to set an example for the world by protecting ALL online content even as it attempts to provide remedies to those who are the victims of online piracy.

Sincerely,

Laura W. Murphy
Director, Washington Legislative Office

Michael W. Macleod-Ball
Chief of Staff/First Amendment Counsel

BROOKINGS

Paper | November 15, 2011

Cybersecurity in the Balance: Weighing the Risks of the PROTECT IP Act and the Stop Online Piracy Act

By: Allan A. Friedman

Executive Summary

Cybersecurity has dominated headlines and the attention of American policymakers. The challenge is not in recognizing the problem, but in understanding how to balance cybersecurity efforts with other policy priorities and scarce resources. Two new bills designed to combat foreign websites that infringe on American intellectual property present one of the first such decisions to Congress: how can we balance the defense of cyberspace and defense against online piracy when the two conflict?

The Senate bill S.968, or the PROTECT IP Act, and the House bill H.R. 3261, the Stop Online Piracy Act, have raised a great deal of controversy. This paper does not deal with the questions of economic value, free expression or other issues raised by advocates on both sides. Instead, I highlight the very real threats to cybersecurity in a small section of both bills in their attempts to execute policy through the Internet architecture. While these bills will not "break the Internet," they further burden cyberspace with three new risks. First, the added complexity makes the goals of stability and security more difficult. Second, the expected reaction of Internet users will lead to demonstrably less secure behavior, exposing many American Internet users, their computers and even their employers to known risks. Finally, and most importantly, these bills will set back other efforts to secure cyberspace, both domestically and internationally. As such, policymakers are encouraged to analyze the net benefits of these bills in light of the increased cybersecurity risks.

Risks of Tampering with the Network

The Domain Name System (DNS) is a critical part of the Internet infrastructure, not just for the user seeking to access web pages, but for almost any operation, research question or network maintenance tool used to cross between organizational and network boundaries. Some interference with the DNS is not unheard of, but it should be done only after careful consideration, and with the full participation of Internet stakeholders.

The bills call for operators of DNS resolvers to "prevent the domain name described in the order from resolving." This is, in effect, lying. As we shall see below, this may sometimes be acceptable, but again must be done with care so as not to interfere with other aspects of network operation.

The broader Internet community has had the chance to judge the appropriateness of other attempts to return misleading results. Some network operators take advantage of imperfectly typed URLs to direct users to a

landing page, rather than return the expected error message Non-Existent Domain (NXDOMAIN). A browser receiving the result NXDOMAIN might return an error "server not found." With a DNS redirect, however, the user is taken to a search page that may assist her, but may also display advertisements. One vendor who enables this capacity claims that a service provider can earn $1-3 per subscriber with this service.[i] While DNS redirect for this purpose is not uncommon, many Internet experts do not view it favorably. Internet Corporation for Assigned Names and Numbers' (ICANN) Security and Stability Advisory Committee (SSAC) cautioned that interfering in DNS responses "can create unpredictable responses,"[ii] and another ICANN advisory group concluded that the practice "create[s] a reasonable risk of a meaningful adverse effect on security and stability."[iii] The SSAC has recommended that new top level domains be prohibited from using redirection.[iv] Clearly, this practice is viewed with apprehension by the body governing the domain name system.

Part of the threat of redirects is the potential for malicious misuse. The DNS system is based on trust between resolution servers. If an intermediary between the client and the authoritative server is untrustworthy, they can inject an incorrect record, diverting the client to a server other than the intended Internet resource. To make this system more trustworthy, the Internet Engineering Task Force (IETF) developed the Domain Name System Security Extensions (DNSSEC), which uses a set of chained cryptographic signatures to establish trust between the authoritative name server (such as the .com servers) and the recursive resolving servers used to translate from a desired URL to the IP address. This protocol allows correct responses to be provably valid, and incorrect responses to be identified as false. DNSSEC is seen as a needed security improvement for the Internet by both technical experts and the U.S. government. U.S. officials have viewed DNSSEC as important for its own systems, as well as the commercial Internet, since at least 2003. Deployment is proceeding slowly, but with the coordination and support of public and private efforts.

Because DNSSEC is designed to prevent malicious redirection of DNS traffic by verifying that DNS responses have not been tampered with, other forms of redirection will break the assurances from this security tool. Engineers from Comcast, in a circulated IETF working paper, clearly state, "It is critically important that service providers understand that adoption of DNSSEC is technically incompatible with DNS redirect."[v] If the client is configured to recognize DNSSEC responses, any intercept will trigger the responses of an attempted man-in-the-middle attack. For the purposes of the bills in this paper, this response may be thought to have little policy impact since the goal is to prevent access in the first place. There are two adverse consequences, however. The first is that, without a reliable and standardized warning mechanism, the user may be unable to distinguish between malicious and illegal resources. The second is that one acceptable response to a DNSSEC failure is to query other recursive resolvers to confirm that the resource is not valid and available. This could violate the goals of the bills since these servers may be outside the jurisdiction of the United States.

It is important to acknowledge that DNS redirection may not always be bad for cybersecurity. Indeed, some domains are known to be security risks, hosting malware or serving as a critical link in the communication and coordination of botnets. As researchers identify which domains pose risks, DNS administrators may want to block them. A new tool called Response Policy Zones (RPZ) allows administrators to select lists of domains with bad reputations (assembled by anyone they might trust) and block their users.[vi] RPZ,

designed to counter malicious behavior online, essentially creates the functionality called for in the bills to block domains specified by a trusted third party, with the potential to redirect the browser to an arbitrary notice page. However, there are key differences between RPZ and the bills' proposals.

First, RPZ engineers acknowledge that, as it exists, there is no easy way to make RPZ work well with DNSSEC. This will ultimately require some modification to DNSSEC to incorporate the error messages following an intercepted query. But because DNSSEC will take some time to fully deploy at the user level, there will be time to explore the most efficient means to implement this change. And because these protocols are implemented in voluntarily by network administrators trying to maximize the security of their networks, an appropriate balance can be found by each administrator.

Second, the legal mandate for the bills' block-list increases the complexity of the DNS network administration. PROTECT IP applies to every "operator of a non-authoritative domain name system server," including local ISPs and even small businesses that run their own networks. Each network must have the capacity to easily alter what can be accessed on their network, regardless of the preferences of the network administrator and her resources and capacities. Security expert Susan Landau observes that adding points of insertion or observation can dramatically alter the security of a system.[vii] Perhaps the largest difference, of course, is that RPZ is voluntary—and ideally in the interest of the user. In a competitive market, users who find one service provider's implementation too broad or narrow can go to another. If the users do not believe that a black list is in their interest, they will find ways around it, as explored below.

Tinkering with DNS by mandating false responses may not break the Internet, but it certainly bends it, and introduces new complexities. The security community understands that these risks must be carefully studied before there is widespread deviation from the accepted standards.

Unintended Consequences Introduce New Risks

By preventing American users from accessing foreign websites, the bills' clear aim, insofar as they deter Americans from supporting behavior that infringes on intellectual property, is to stop piracy. Past efforts to halt piracy do sometimes have limited success, but they also succeed in changing the behavior of millions of Americans to find other means of accessing this content. Any analysis of these bills must therefore explore the consequences of these new behaviors. The DNS blocking of foreign websites is not only trivial to defeat, but many work-arounds will definitely have dangerous unintended consequences.

The bills seek to block access to foreign infringing websites by preventing American domain name servers from translating the infringing domain name into its Internet address. This is trivial to defeat on many levels, as has already been chronicled widely.[viii] One of the easiest and most direct methods is simply to use a DNS server that is located outside of the bills' jurisdiction in another country. This requires minimal computer expertise.[ix]

Before exploring the harms of using a non-trusted DNS server, is there any reason to expect users to change their behavior en masse? The data says yes. Those seeking infringing content have always responded to legal and technical countermeasures by shifting their habits. From Napster to Kazaa to LimeWire to BitTorrent to illegal streaming websites, users adapt by the millions. When the RIAA succeeded in shutting down the peer-to-peer client LimeWire in 2010, use of a similar client FrostWire more than

doubled within 3 months.[x] When Sweden passed a law requiring service providers to turn over identity information on infringers, demand for both paid and unpaid anonymity services skyrocketed "beyond all expectations."[xi] It would be incredibly naïve to expect anything other than attempts to evade DNS blocking, and using DNS servers outside the U.S. is the easiest path.

This introduces huge risks to American Internet users. These DNS servers can sit as the "man-in-the-middle" on all Internet transactions, allowing the possible compromise of almost any Internet transaction. The attacker can pass along the legitimate website during the attack, preventing the user from realizing that an attack is ongoing. Even the use of encryption (such as SSL or https) will not help. The attacker can not only compromise web traffic, but email as well. There already exists malware that forces victims to use remote, rogue DNS servers to maliciously redirect traffic to key financial websites.[xii] The operators behind these attacks will undoubtedly seek to gain further traffic to these servers.

The risks of malware, financial fraud and espionage will not fall exclusively on the users guilty of infringement. Rather, they will be shared by anyone who shares a network with these users. It is easy to imagine a teenager altering the family PC to access a foreign infringing domain, but leaving the computer compromised for the family's other uses, including banking, accessing government websites and even work.

Even if the foreign DNS servers are benign and supervised by an open source community, there is still a destabilizing effect. Content Deliver Networks (CDNs), such as Akamai, that make it easier and cheaper to send large files over the Internet by replicating it many times across the Internet. Some CDNs use the DNS request to determine the closest and most efficient content server.[xiii] Foreign domain requests will confuse this system, leading to greater inefficiencies and instability. Interestingly enough, this can lead to slower content deliver from paying, legitimate sites, further increasing the incentives for infringement. ISPs also use local DNS information to better manage their networks; the less complete this data is, the less informed decisions will be.

Cybersecurity Policy

Many cybersecurity issues require international coordination. The GAO has identified 19 international organizations relevant to Internet governance, each with a different set of stakeholders and counter-parties.[xiv] In each forum, the United States must be seen as a good faith actor, seeking to promote global security in cyberspace without advancing alternate agendas. The policies must not be perceived as conflicting with other values, such as openness and limited governance. While many would agree that any measure is acceptable to prevent intellectual property infringement, some might see this as a signal of what values the U.S. will emphasize—and what it will implicitly devalue. As the Council on Foreign Relations' Rob Knake notes, "If the United States fails to provide the leadership necessary to address the security problems, other states will step in."

It is important to remember that the United States occupies a unique position in Internet governance. The Internet was invented here, and many of its key institutions remain affiliated with the federal government. U.S. companies support much of the Internet architecture. This dominant position has not gone unnoticed from those who would prefer a more globally representative governing structure. This would necessarily involve reducing U.S. influence in key security-relevant bodies.

American representatives across the government have worked hard to focus the international dialogue on "cybersecurity," without permitting discussion to be reframed as "information security," which can include policing of content instead of just actions. This position is undermined by domestic bills that focus on content at the expense of cybersecurity. It will be hard to argue with other nations that discussions should focus on preventing malicious behavior, rather than stamping out illegal content—a category into which many other nations put political speech. Indeed, other observers have pointed out the challenges in reconciling these anti-infringement bills with America's stated agenda of Internet Freedom, particularly SOPA's anti-circumvention prescriptions.

Lastly on the international front, it is important to remember the difficulties in perfectly mapping the Internet to national boundaries. It is highly likely that DNS blocking will spill over into other countries. In 2010, China's internal attempts to block certain websites via DNS spilled over to the broader Internet.[xv] The U.S.-China Economic and Security Review Commission's Annual Report to Congress noted, "The implications of China's effort to impose 'localized' restrictions to something as inherently global in scope as the Internet."[xvi] Since the United States' networks are so centrally positioned in the global information infrastructure, there is a good chance that foreign DNS queries will pass through U.S. resolvers. Other countries may object to our unilateral enforcement without adequate international normalization or even discussion.

Domestically, the bills pose three principle risks, based on expectations and trust. First, by mandating an unpopular enforcement mechanism to the ISP, users may grow to trust their ISPs less, even as service providers play an increasingly large role in American cybersecurity policy. If the user is treated as an enemy, it makes winning consumer acceptance for other efforts all the more difficult. A recent proposal from the National Institute of Standards and Technology would have ISPs detect botnets on customers' machines and work with them for remediation. This requires user trust and a belief that user security is a higher priority for the service provider than other business interests. The ISPs also depend on user trust to make the entire network better off. By studying pooled DNS lookups across a large set of users, security researchers can learn a great deal about attacks based on data referred to as Passive DNS. This data will be incomplete if users evade the DNS blocks en masse, as discussed above.

Expectations also drive investment, and new investment can happen under the jurisdiction of these bills, or outside the country. Without engaging in the larger debate of how this bill will impact long-term economic growth, there is a security issue in jurisdiction. If the provisions in the bills that allow rights holders to go after domestic assets drive these assets offshore, they can make the fight against other illegal digital activities harder to pursue. As new Top Level Domains are issued by ICANN, their supporters may push for offshore control. Similarly, if attacks against website monetization tools, including ad networks and payment networks become too aggressive, offshore alternatives will emerge. American law enforcement and intelligence will have less leverage over these. If one acknowledges that there are cybercrime issues other than intellectual property infringement, such as child pornography or financial fraud, then a long-term enforcement tradeoff will be made. Making it more efficient to drive potential wrongdoing away from America's jurisdiction may ultimately hinder law enforcement.

Finally, and perhaps most importantly, the bills set a certain expectation with respect to the relative importance of cybersecurity versus industry profitability. There is always a tradeoff between economic

efficiency and security. As technology evolves, each sector of the economy discovers new risks, just as they discover new benefits. These bills offer an explicit tradeoff: protecting the economic value of intellectual property from a narrow type of infringement against a larger and more diffuse set of security priorities.

Cybersecurity policymakers will only encounter this tradeoff more frequently. The costs of the status quo must be measured against the security risks of mandating a change in the Internet architecture. Unfortunately, it is always easier to estimate actual business models than uncertain security risks. This is why market solutions for cybersecurity are particularly challenging.[xvii] If securing the power grid harms the business model of energy companies, will Congress still act to ensure our critical infrastructure is less vulnerable to attack?

Will Cybersecurity Be a Priority?

Threats from cyberspace present serious challenges, yet no one suggests that we turn off the Internet to protect ourselves. Similarly, while digital entertainment is a key part of the economy, few argue that we lock down all networks and devices for perfect enforcement of intellectual property. The question is where the balance will be struck.

The risks from the proposed policies are diffuse, and the harms of a perturbed ecosystem, exposed Americans and a more difficult cybersecurity agenda lie in the future. Yet they are real—and will have concrete, negative impacts on our nation's ability to defend itself, endangering everyone from the average user to shapers of international policy. This will be the first legislation that pits our cybersecurity priorities against entrenched economic interests, highlighting a very real social choice. Congress' actions on PROTECT IP and SOPA will offer some insight into whether policymakers are genuinely prepared to take cybersecurity seriously.

[i] Xerocole Solutions. http://www.xerocole.com/solutions/

[ii] "SAC 032 Preliminary Report on DNS Response Modification," ICANN Security and Stability Advisory Committee, June 2008; www.icann.org/en/committees/security/sac032.pdf.

[iii] ICANN Registry Services Technical Evaluation Panel Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal (2006)

[iv] "SAC041: Recommendation to Prohibit Use of Redirection and Synthesized Responses by New TLDs," ICANN Security and Stability Advisory Committee (2009) www.icann.org/en/committees/security/sac041.pdf.

[v] Creighton, T., Griffiths, C., Livingwood, J., and Weber, R. "DNS Redirect Use by Service Providers. Internet Draft draft-livingood-dns-redirect-03." (2010) http://tools.ietf.org/html/draft-livingood-dns-redirect-03

[vi] ISC. BIND 9 Administrators Reference Manual, 2011. See 6.2.16.19 and 6.2.16.20

[vii] Landau, Susan. Surveillance or Security? The Risks Posed by New Wiretapping Technologies. MIT Press, 2011

[viii] See, e.g., Wilson, Drew. "8 Technical Methods That Make the PROTECT IP Act Useless." www.zeropaid.com/news/95013/8-technical-methods-that-make-the-protect-ip-act-useless/

[ix] See, e.g., http://windows.microsoft.com/en-US/windows7/Change-TCP-IP-settings.

[x] Sandoval, Greg. "Study: LimeWire demise slows music piracy" http://www.news.cnet.com /8301-31001_3-20046136-261.html

[xi] Simpson, Peter Vinthagen. New law increases demand for anonymous web surfing www.thelocal.se/18658/20090403/#

[xii] David Dagon, Chris Lee, Wenke Lee, Niels Provos . "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority", , Proc. 15th Network and Distributed System Security Symposium (NDSS), 2008.

[xiii] Vixie, Paul. What DNS is Not. ACM Queue, 2009. http://queue.acm.org/detail.cfm?id=1647302.

[xiv] Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606 July 2, 2010

[xv] Zmijewski, Earl. "DNS: When Governments Lie." http://www.renesys.com/blog/2010/11/dns-when-governments-lie-1.shtml

[xvi] USCC. 2010 Annual Report to Congress. http://www.uscc.gov/annual_report /2010/Chapter5_Section_2(page236).pdf

[xvii] Friedman, Allan. Economic and Policy Frameworks for Cybersecurity Risks. (2011) www.brookings.edu/papers/2011/0721_cybersecurity_friedman.aspx

Author

Allan A. Friedman
Fellow, Governance Studies
Research Director, Center for Technology Innovation
@allanfriedman

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper describes technical problems raised by the DNS filtering requirements in S. 968, 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 Labovitz, "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.

---

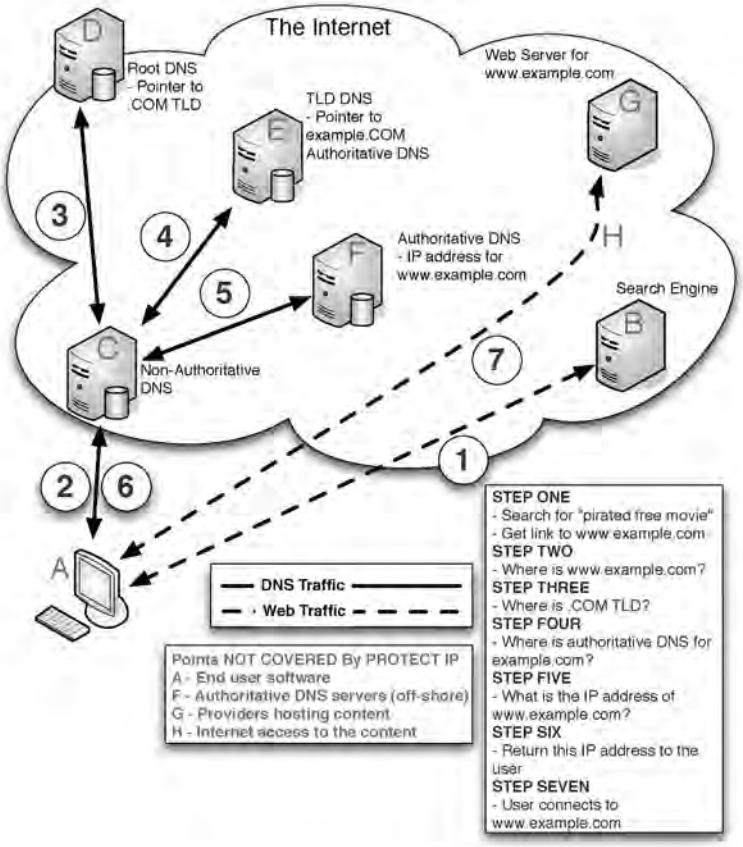
[23] Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *InformationWeek*, February 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/229218959.

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



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.

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.

November 15, 2011

Commentary on S.968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011; and H.R.3261, the Stop Online Piracy Act.

The Anti-Phishing Working Group (APWG.org) is an industry association focused on eliminating identity theft and fraud on the Internet. The APWG has over 1,500 member companies and agencies representing financial institutions, security companies, ISPs, e-commerce companies and law enforcement agencies.

Since 2003, the APWG and its members have been fighting fraud, theft and impersonation on the Internet, which has cost US companies billions of dollars in direct and indirect financial losses.

As an industry group of over 1,500 companies, we support the rights of copyright holders to protect their works. However, in our examination, the PROTECT IP bill in the Senate, and it's House counterpart, the "Stop Online Piracy Act," propose technological regulations that would not only impede security on the Internet, but that would potentially result in new kinds of financial fraud against consumers and businesses in the United States.

Requiring U.S.-based DNS providers to re-route the Internet traffic of consumers of infringing content will have the unintended consequences of driving consumers to non-U.S.-based DNS providers. These providers can easily reroute requests to online banking and e-commerce sites to criminal websites located outside of the United States. This will create a new cyber crime fraud economy that will threaten e-commerce and banking in the United States. Additionally, the proposed technical measures requiring DNS providers to reroute traffic will break the improved Internet security measures that the Department of Homeland Security has been working towards for many years (DNS-SEC), in conjunction with the Internet and Security industries.

Therefore the APWG Board of Directors and Steering Committee expresses our disagreement with the proposed PROTECT IP bill and the Stop Online Piracy Act.

Again, we support the rights of copyright holders, but we believe that this proposed legislation will create technological problems on the Internet that will result in new kinds of cyber crime and a reduction in the security of the Internet. We recommend that this bill not be approved, and that a more carefully considered approach be taken that will consider the after-effects of such legislation. It is in the best interests of everyone in the United States that we protect the security not only of our copyrighted materials, but also of our banking and e-commerce systems.

David Jevans
Chairman, Anti-Phishing Working Group
Cambridge, MA
USA 02140

Opinion: Copyright bills could kill hopes for secure Net

By STEWART BAKER | 11/16/11 5:36 AM EST

Everyone knows that Internet security is bad and getting worse. Recognizing the problem, Congress is hard at work on cybersecurity, with a number of bills on the table. Ironically, at the very same time, Congress is getting ready to pass a copyright enforcement bill that could kill our best hope for actually securing the Internet.

How did that happen? Let's start with the Internet, where fake websites cost users millions of dollars in fraud losses every year. Unless we find a better system for locking down website identities, this and other forms of online crime will continue to skyrocket.

It turns out that Internet engineers have already designed a system to solve this problem — a set of technical rules that go by the unlovely name of DNSSEC. Under these rules, an Internet website will be given identification credentials by the same company that registers its Internet name. Thus, when Citibank claims the domain name Citibank.com, the registry who issues the name will at the same time lock that name to a particular Internet address. From then on, anyone who types "Citibank.com" into his browser will be sent to one and only one Internet address. Under the new system, the browser simply will not take the user to a site that isn't verified by Citibank's unique credentials.

That's protection that the people who bank online need today.

Why don't they have it? Two reasons. The first is friction. Moving to the new rules won't be free. It will require a lot of work by browser companies, Internet service providers, domain registries and others — many of whom may never get any direct benefit from the change. Naturally, these companies are a little slow to spend money that just makes the Internet overall safer; that's the tragedy of the commons. But as the need for security becomes obvious to all, we're slowly overcoming that friction, thanks in part to the leadership of my old agency, the Department of Homeland Security, in getting government to adopt the new procedures.

The second problem is new. It is Hollywood's desperate desire to keep foreign websites from delivering pirated movies and music to American computers. To do that, the movie industry wants a law that will require Internet service providers block their customers from going to those sites. Instead, the users are supposed to be sent to a site that warns them against copyright infringement.

Hollywood has sold that idea to Congress, and bills are now moving through both houses to impose this "block and redirect" obligation on Internet service providers. And they're moving fast. The Senate bill is out of committee, while the House Judiciary Committee is holding hearings on a similar bill Wednesday.

This is far faster than Congress's cybersecurity effort, and it runs directly counter to that effort. Because "block and redirect" is exactly what crooks are doing today to bank customers. If the bills become law, the security system won't be able to tell the difference between sites that have been blocked by law and those that have been sabotaged by hackers. Indeed, it isn't hard to imagine crooks redirecting users to sites that say, "You were redirected here because the site you asked for has violated copyright," while at the same time planting malware on the user's computer.

What's more, the bill will likely break the fragile consensus that my former agency, the Department of Homeland Security, has spent years helping to build around the switch to DNSSEC. If the bill passes, practically everyone who needs to make changes to implement DNSSEC will instead be on the phone to their lawyers asking whether they could be sued for adopting a security technology that will make the mandated "block and redirect" system even more difficult.

If "block and redirect" could stop Hollywood's bleeding, perhaps a case could be made for undermining everyone's security in order to protect the studios' intellectual property. But it won't stop the bleeding. Even today, if someone is blocked and redirected away from his favorite pirate website, he can find many simple ways to defeat the block. He can paste his favorite pirate website's number (rather than its name) into the address box on his browser. Or he can simply tell his computer to look up the site's address on a Canadian server instead of an American one. There are many more.

Passing this bill will make Hollywood feel better and richer. For about a minute. It will leave the rest of us hurting and poorer for years.

Stewart Baker, former DHS Assistant Secretary for Policy and former NSA General Counsel, is currently a partner at Steptoe & Johnson in D.C. His 2010 book, Skating on Stilts, examined privacy issues as they relate to homeland security.

November 15, 2011

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

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

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

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

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

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

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

One issue merits special attention. We are very concerned that the bills as written would seriously undermine the effective mechanism Congress enacted in the Digital Millenium Copyright Act (DMCA) to provide a safe harbor for Internet companies that act in good faith to remove infringing content from their sites. Since their enactment in 1998, the DMCA's safe harbor provisions for online service providers have been a cornerstone of the U.S. Internet and technology industry's growth and success. While we work together to find additional ways to target foreign "rogue" sites, we should not

jeopardize a foundational structure that has worked for content owners and Internet companies alike and provides certainty to innovators with new ideas for how people create, find, discuss, and share information lawfully online.

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

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

Thank you in advance for your consideration.

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

Harvard Business Review

HBR Blog Network

The Great Firewall of America

by James Allworth | 9:31 AM October 28, 2011

The Senate's PROTECT IP Bill, designed to stop piracy, now has a matching bill in the House: E-PARASITE. It would have been tough to top PROTECT IP, but they've managed to do it. It contains provisions that will chill innovation. It contains provisions that will tinker with the fundamental fabric of the internet. It gives private corporations the power to censor. And best of all, it bypasses due legal process to do much of it.

The timing could not be more exquisite. In the midst of protests emerging all around the US complaining about the power that corporations have inside our political system, big content is quite literally trying to foist its own version of the Great Firewall of China on to the American public.

So what's in the bill?

First, the US Government will set up a blacklist of international sites that it says are infringing IP rights. Regardless of whether the ISP believes the Government has it right or not — and the Government has already got it seriously wrong (http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/) before — ISPs must comply with all sites that the US Attorney General lists. If they don't, they lose their safe harbor provisions. That is the equivalent of making phone carriers liable for conversations that are being made on their phone lines. But more broadly, this blacklist concept may sound familiar to you: it's been borrowed from China. The Government decides what you can and can't see on the web. ISPs have to comply with it, or they're liable.

Second, the technical way this is to be achieved is by tinkering with Domain Name Servers, the technology that translates "http://www.hbr.org (http://hbr.org/) " into the unique IP address where a server is stored. Given the DNS is at the heart of the internet, pulling at this fabric will have some dramatic consequences. If internet users in the US don't get the results they're looking for using American DNS servers, they're simply going to go overseas instead. Amongst many other issues, Dan Kaminsky, chief scientist at security vendor DKH points out (http://www.cio.com/article/686212 /Engineers_PROTECT_IP_Act_Would_Break_DNS) : "It's not just that lookups to the Pirate Bay go overseas; lookups to Bank of America go overseas. This is handing over American Internet access to entities we explicitly do not trust, entities that are unambiguously bad guys."

Third, the Digital Millennium Copyright Act (http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act) (DMCA), introduced over a decade ago and designed to balance IP rights with the technology innovation that has boomed in the US, is being modified to the point of being lopsided. Previously, if a rights holder believed a site was infringing content, they could send a takedown notice and the content would be removed or the takedown could be contested. But the E-PARASITE update is outrageous. Payment providers (Paypal, Visa, Mastercard) and ad networks would be required to terminate services to any site upon receipt of a letter merely alleging that the site is "dedicated to the theft of US property." In short, rights holders can turn the funds off something they don't like, and the funds won't turn back on until after it has gone through the courts. In the meantime: no income. Imagine that every time somebody was sued, they stopped receiving paychecks. That would make it kind of difficult to find the money to pay their lawyer, right? That is what this bill would do.

Supporters of the bill say that it won't target legitimate sites. Let's look at the language. A site is "dedicated to the theft of US property" if it is a US-directed site (i.e. can be accessed in the US) that: "is taking, or has taken deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute a violation of section 501 or 1201 of title 17, United States Code." Now I'm not a lawyer, and this language seems to have been crafted to defeat reading by a regular human being. But the short version is: if the site can be used to infringe, and doesn't take steps to prevent against the

"high probability" that it will, then a site can be declared dedicated to the theft of US property. I'm not sure if the drafters of this legislation have used the internet before, but that's everything. Facebook. Google. Tumblr. eBay. Wikipedia. As TechDirt put it: any site that has user-generated content (http://www.techdirt.com/articles/20111027/00083116531/e-parasites-bill-end-internet-as-we-know-it.shtml) . And think that it won't chill innovation? You may have heard that Viacom has been suing Youtube for exactly this (and so far, not doing too well). Under this bill, YouTube would not have been able to generate any revenue while the court case was ongoing. And Monster Cable — a big supporter of this bill — has labelled both Craigslist and eBay infringers (http://www.techdirt.com/articles/20111005/10082416208/monster-cable-claims-ebay-craigslist-costco-sears-are-rogue-sites.shtml) .

Is this really what we want to do to the internet? Shut it down every time it doesn't fit someone's business model?

But even this isn't the most troubling aspect of the bill. There is the broader message America would be sending to the rest of the world: that it's OK for Governments to set up internet censorship apparatus. Given the Arab Spring, given Occupy Wall Street, given all the effort America has put into fighting internet censorship across the globe (http://www.dailyfinance.com/2010/01/21/clinton-assails-censorship-unveils-new-u-s-internet-freedom-po/) is this really the message the US should be broadcasting right now?

This is terrible legislation. The congresswoman from Silicon Valley, Rep. Zoe Lofgren, yesterday described (http://news.cnet.com/8301-31921_3-20126590-281/rep-lofgren-copyright-bill-is-the-end-of-the-internet/) the effect this bill will have: "from what I've already read, this would mean the end of the Internet as we know it". The U.S. is in a jobs crisis, and one of the few bright spots on the horizon are tech firms like Facebook and Twitter. Make no mistake: this bill threatens their very existence. At best, it will send them fleeing overseas. And for what? To prop up the business model of an industry in the midst of disruption. It's happened time and time again: the most famous example is Jack Valenti trying to ban the VCR (http://cryptome.org/hrcw-hear.htm) , claiming it was to the movie industry what the Boston Strangler was to women at home. We know how that one turned out: the VCR lived, and the movie industry went on to generate profits unlike it had seen ever before.

This is history repeating. Except the remedy big content (http://blogs.hbr.org/cs/2011/03/big_content_is_strangling_amer.html) are proposing this time wouldn't just stop VCR technology. It would chill free speech, stop innovation, and pull at the fabric of the internet. In short: they are trying to give America it's very own version of the Great Firewall of China.

Ms. LOFGREN. You know, I think some today have sort of written off, I think, serious criticisms of this bill as hyperbole, and that the only objection is about money and hyperbole, and I just do not think that is the case. The big tech companies were not the ones who said this bill would cause the U.S. to lose its position as a global leader in supporting a free and open Internet. That is from dozens of human rights groups around the world. The big tech companies were not the ones that wrote that the bill has the potential

to do consumers more harm than good. That is from the Consumer Union and other nonprofit consumer groups.

The big tech companies did not write that the bill is in conflict with the First Amendment. That is from the ACLU and over 100 law professors. It was not the big tech companies who said the bill would kill our best hope for securing Internet. No, that is from Stewart Baker, the former Assistant Secretary for DHS and the former General Counsel of the National Security Agency. Dozens of venture capitalists, not big tech companies, wrote that the bill will stifle investment and Internet services, throttle innovation, and hurt American competitiveness. And it has not generally been the policy of this Committee to dismiss the views of those in industries that we are going to regulate, and these are just a few of the examples.

Now, I understand why co-sponsors of the legislation are not happy about widespread criticism of the bill, but I think impugning the motives of the critics rather than engaging in the substance is a mistake.

I have a number of questions, and I note that, yeah, we have got six witnesses here. Five are in favor and only one is against, and that troubles me. I will just say that. You know, I do not think it is a balanced effort, and I am sorry that we do not have any technical expertise on this panel in terms of engineering talent, because I think that is an important issue as to the DNS blocking portions of the bill.

So, let me ask a question of Mr. O'Leary. Do you believe that software programs should be illegal if they allow a user to circumvent Internet filtering ordered by the government?

Mr. O'LEARY. I do not believe that software programs should be per se illegal. I think if people misuse them, then they should be. If they misuse any product in violation of a law, they should suffer the consequences.

Ms. LOFGREN. So, the ability to just simply circumvent the takedown order as a software add-on to a browser should continue to be illegal?

Mr. O'LEARY. Well, no. If you are saying you are building something and specifically to avoid an order of the court not to do something, I do have a problem with that.

Ms. LOFGREN. So, you think that software ought to be illegal.

Mr. O'LEARY. Well, that is not what I said, no.

Ms. LOFGREN. Well, it is one or the other. Either you should be able to do that, or you should not be able to do it. Which is it?

Mr. O'LEARY. Does the software have a legitimate purpose, or is it simply to circumvent a court order?

Ms. LOFGREN. Well, circumventing software can be a multiplicity of views. For example——

Mr. O'LEARY. Right, but in your question, you said the software would be created to allow circumvention.

Ms. LOFGREN. There is an add-on to Firefox that will allow——

Mr. O'LEARY. I think that most legitimate companies in the United States, including Firefox, should abide by court orders and follow the law.

Ms. LOFGREN. So, well, you are not really answering the question. I will take from here you think that that ought to be regulated at least.

Mr. O'LEARY. Regulated in much the same way as we regulate people driving drunk and stealing things, yeah, I think that—I know that the word "regulation" has——

Ms. LOFGREN. Let me ask you this, because I do not have a long time, and I assume that you were directing your comments that people did not—that Northern California people did not care about jobs in the rest of America, either to myself or Mr. Lungren since we are the only Members of the Committee from Northern California. I will say I do care about jobs all over America. And, in fact, eBay, which is headquartered in San Jose, has enabled thousands of Americans all over the country to form small businesses, and to use the Internet to sell products.

I would like to know, your concept—do you think that this is a big problem? I think it is a problem. I think that Internet piracy is something that is troubling. It is illegal. And I think we need to do something about it. So, let me just put that out there.

How many sites do you think need to be shut down in order to say we have succeeded in the fight against Internet high receipt? Is it a dozen? Is it hundreds? Is it thousands? Do you have any idea the scope of the number of sites that need to be removed?

Mr. O'LEARY. Well, I think, first of all, you've mischaracterized my comment about Northern California, and I would like to correct the record on that. I was simply——

Ms. LOFGREN. Well, do it later, because I do not have that much time. Answer my question, please.

Mr. SMITH. Actually, the gentlewoman's time has expired, but you are free to answer the question.

Mr. O'LEARY. Thank you. The comment about Northern California was in the context of this debate. The perception has been created by opponents of this bill that all of the innovation and all of the creative thinking comes out of Silicon Valley. I was not taking umbrage with anyone in Silicon Valley. We have great relationships with a lot of people in Silicon Valley. Pixar, which makes wonderful movies, is in Silicon Valley. Apple, which is a legitimate online retailer, is in Silicon Valley. I was also making the simple point, Congresswoman, that there are people all over this country in places like Detroit, Baltimore, Texas, North Carolina——

Ms. LOFGREN. Mr. Chairman, I wonder since——

Mr. SMITH. The gentlewoman——

Mr. O'LEARY. I would be happy to answer your question.

Ms. LOFGREN. May I have an additional 30 seconds?

Mr. SMITH. Well, the gentleman—answer the question very briefly.

Ms. LOFGREN. How many sites?

Mr. O'LEARY. Well, I know for a fact that we could start with Pirate Bay, which was mentioned earlier. I do not know how many——

Ms. LOFGREN. So, is it just Pirate Bay, do you think, or do you think it is a dozen? Is it 100? Is it 1,000? What do you think?

Mr. O'LEARY. It would be easier to answer the question if I was allowed to. There are multiple sites out there. This is a legitimate

problem. We have been very clear, and we will continue to be clear, that there is no silver bullet. The problem is evolving and changing. I cannot sit here right now and tell you in good faith that I know what that number is, but what I do know is that there are literally hundreds of sites out there that are engaging in this activity. And all you need to know that——

Ms. LOFGREN. Do you think it is in the neighborhood of——

Mr. SMITH. The gentlewoman's time——

Mr. O'LEARY [continuing]. Know that is to go to Google and type in J. Edgar, and you will get a list of page after page after page——

Ms. LOFGREN. Or Baidu, or Bing, or any of them.

Mr. O'LEARY [continuing]. Of sites that are engaging in this illegal activity.

Ms. LOFGREN. So, it is hundreds of thousands.

Mr. SMITH. The gentlewoman's time has expired, but let me remind Members that they are welcome to submit written questions to any of the panelists, and we will try to get those answers to the Members quickly as we can.

The gentleman from California, Mr. Issa, is recognized?

Mr. ISSA. Thank you, Mr. Chairman. And the gentlelady from the North, while I am deep in the Confederacy of California, went through quite a litany of good opponents to the bill. I would like to add to that, by unanimous consent, the following: a joint letter by 160 entrepreneurs, founders, and CEOs, and executives; a letter expressing concern about SOPA from the Digital Media Association; a statement by the Consumer Electronics Association, which was denied an opportunity to be here as a witness; a letter signed by 53 venture capitalists expressing concern regarding the Protect Act; and a transcript of recent remarks made by Vice President Joe Biden that he gave at the London Cybersecurity Conference germane to his concerns about this bill.

Mr. SMITH. Without objection.

[The information referred to follows:]

To Members of the United States Congress:

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

It is a truism that small businesses create significant economic growth and jobs, but it is more accurate to say that *new* businesses, including tech start-ups, are most important.[1] The Internet is a key engine of today's economy,[2] and much of its economic contribution is attributable to companies that did not even exist 10 or even 5 years ago. The Internet has also created new opportunities for artists and other content creators -- today, there is more content being created by more people on more platforms (including some of our businesses) than ever before.
We are not opposed to copyright or the bill's intent, but we do not think this bill will actually fulfill copyright's purpose of encouraging innovation and creativity. While the bill will create uncertainty for many legitimate businesses and in turn undermine innovation and creativity on those services, the dedicated pirates who use and operate "rogue" sites will simply migrate to platforms that conceal their activities.

Our concerns include the following:

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

  PIPA provides a new weapon against legitimate businesses and "rogue" sites alike, and the concern in this context is not merely historical or theoretical. Recent press reports noted that advertising giant WPP's GroupM subsidiary had put together a list of 2,000 sites that were declared to be "supporting piracy," on which none of its advertising would be allowed to appear. That list - which was put together with suggestions from GroupM clients - includes Vibe.com, the online version of the famed Vibe Magazine, founded by Quincy Jones, and a leading publication for the hip hop and R&B community. It also included the Internet Archive's Wayback

Machine, which preserves copies of Web pages in order to fill a similar function as libraries.
When a famous magazine and a library get lumped in with "rogue pirate sites" in this way, it's not hard to see how an overzealous copyright holder might seek to shut legitimate businesses down through PIPA.

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

  PIPA would put new burdens and possible liability on independent third parties, including payment processors, advertising firms, information location tools and others. The definitions here are incredibly vague, and many companies signed below could fall under the broad definitions of "information location tools," meaning costly changes to their infrastructure, including how we remain in compliance with blocking orders on an ever-changing Internet.

  Separately, including a private right of action means that any rightsholder can tie up a service provider in costly legal action, even if it eventually turns out to not be valid. Given the broad definitions used above for sites "supporting piracy," it's not difficult to predict that plenty of legitimate startups may end up having to spend time, money and resources to deal with such actions.

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

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

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

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

greater than the challenges, and the best way to address the latter is to create more of the former.

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

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

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

Asheesh Advani
Covestor, Virgin Money USA, CircleLending

David Albert
Hackruiter

Will Aldrich
SurveyMonkey, TripIt, Yahoo

Courtland Allen
Syphir, Tyrant

Lloyd Armbrust
OwnLocal.com

Jean Aw
NOTCOT Inc.

Joshua Baer
Capital Factory, OtherInbox, UnsubCentral, SKYLIST

Andy Baio
Upcoming, Kickstarter

Edward Baker
Friend.ly

David Barrett
Expensify

Jonathan Baudanza
beatlab.com, Rupture

Katia Beauchamp
Birchbox

Idan Beck
Incident Technologies

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

Derek Dukes
Stealth Startup, Dipity, Yahoo!

Jennifer Dulski
The Dealmap

Rod Ebrahimi
ReadyForZero, DirectHost

Chas Edwards
Luminate, Digg, Federated Media, MySimon

Dale Emmons
Vidmakr

David Federlein
Fowlsound Productions, Soapbox Coffee, Inc.

Mark Fletcher
ONElist, Bloglines

Andrew Fong
Kirkland North

Tom Frangione
Simply Continuous, Telphia

Brian Frank
Live Colony

Ken Fromm
Vivid Studios, Loomia, Iron.io

Nasser Gaemi
BigDates, ASAM International

Matt Galligan
SimpleGeo, SocialThing

Zachary Garbow
Funeral Innovations

Jud Gardner
Comprehend Systems

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

Christopher Golda
BackType

Eyal Goldwerger
TargetSpot, XMPie, WhenU, GoCargo

Jude Gomila
Heyzap

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

Steve Greenwood
drop.io

James Gross
Percolate, Federated Media

Sean Grove
Bushido, Inc.

Anupam Gupta
Mixpo

Mike Hagan
LifeShield, Verticalnet, Nutrisystem

Tony Haile
Chartbeat, Chi.mp

Jared Hansen
Breezy

Scott Heiferman
Meetup, Fotolog

Jack Herbeck Jr.
Elroynet, Blu Zone

Eva Ho
Factual, Navigating Cancer, Applied Semantics

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

Jason Huggins
Blu Zone

Ben Ilfeld
Macer Media

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

Jason Jacobs
FitnessKeeper

Daniel James
Three Rings Design

David Jilk
Standing Cloud, eCortex, Xaffire

Noah Kagan
Appsumo, GetGambit

Bill Kallman
Scayl, Varolii

Jon Karl
iovation, ieLogic

Michael Kamjanaprakorn
Skillshare

Bryan Kennedy
Sincerely.com, AppNinjas, Xobni, Pairwise

Derek Kerton
Kerton Group, Telecom Council of Silicon Valley

Drew Kese
Ecount, Orocast
David Kidder
Clickable, SmartRay Network, THINK New Ideas, Net-X

Eric Koger
ModCloth

Kitty Kolding
elicit, House Party, Jupiter

Pete Koomen
Optimizely, CarrotSticks

Brian Krausz
GazeHawk

Amit Kumar
Socialscope

Ryan Lackey
HavenCo, Blue Iraq, Cryptoseal

Jeff Lawson
Twilio, Nine Star, Stubhub, Versity

Peter Lehrman
AxialMarket, Gerson Lehrman Group

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

Michael Lewis
Stellar Semiconductor, Cryptic Studios

Thede Loder
Boxbe, Leverage Information Systems

Marissa Louie
Ness Computing, HeroEX, AD-Village

Eric Marcoullier
OneTrueFan, Gnip, MyBlogLog, IGN

Michael Masnick
Floor64

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

Dwight Merriman
DoubleClick, BusinessInsider, Gilt Groupe, 10gen

Scott Milliken
MixRank.com

Michael Montano
BackType

Dave Morgan
Simulmedia, TACODA, Real Media

Zac Morris
Caffeinated Mind Inc.

Rick Morrison
Comprehend Systems

Amy Muller
GetSatisfaction, Rubyred Labs

Darren Nix
Silver Financial

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

Craig Ogg
ThisNext, Stamps.com, TrueCar

Alexis Ohanian
Breadpig, Hipmunk, Reddit

Casey Oppenheim
Disconnect, Oppenheim Law

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

Michael Ossareh
Heysan

Gagan Palrecha
Chirply, Zattoo, Sennari

Scott Petry
Authentic8, Postini

Mark Pincus
Zynga, Tribe Networks, SupportSoft, FreeLoader

Chris Poole
4chan, Canvas

Jon Pospischil
PowerSportsStore, AppMentor, FoodTrux, Custora

Jeff Powers
Occipital

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

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

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

Vikas Reddy
Occipital

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

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

Avner Ronen
Boxee, Odigo

Zack Rosen
ChapterThree, MissionBicycle, GetPantheon

Oliver Roup
VigLink

Slava Rubin
IndieGoGo

David Rusenko
Weebly

Arram Sabeti
ZeroCater

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

Geoff Schmidt
Tuneprint, MixApp, Honeycomb Guide

Sam Shank
HotelTonight, DealBase, SideStep, TravelPost

Upendra Shardanand
Daylife, The Accelerator Group, Firefly Network

Emmett Shear
Justin.tv

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

Chris Shipley
Guidewire Group

Adi Sideman
Oddcast, Ksolo Karaoke, TargetSpot, YouNow

Chris Sims
Agile Learning Labs

Dan Siroker
Optimizely, CarrotSticks

Rich Skrenta
Blekko, Topix, NewHoo

Bostjan Spetic
Zemanta

Joel Spolsky
StackExchange, Fog Creek Software

Josh Stansfied
Incident Technologies

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

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

Jack Templin
Lockify, ARC eConsultancy

Craig Tumblison
Bitcove

Khoi Vinh
Lascaux, NYTimes.com, Behavior Design

Joseph Walla
HelloFax

Brian Walsh
Castfire, Three Deep
David Weekly
PBWorks

Jack Welde
Smartling, eMusic, RunTime Technologies, Trio Development

Evan Williams
Blogger, Twitter, Obvious

Holmes Wilson
Worcester LLC, Participatory Culture Foundation

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

Dennis Yang
Infochimps, Floor64, CNET, mySimon

Chris Yeh
PBWorks, Ustream, Symphoniq

Kevin Zettler
Bushido, Inc.

November 16, 2011

Chairman Lamar Smith
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member John Conyers Jr.
House Committee on the Judiciary
B-351 Rayburn House Office Building
Washington, D.C. 20515

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

Dear Chairman Smith and Ranking Member Conyers:

As the leading national trade association dedicated to representing the interests of legitimate online distributors of digital music, movies and books, the Digital Media Association ("DiMA") remains deeply committed to eliminating acts of online copyright infringement. DiMA members collectively spend more than a billion dollars annually to license the right to perform, distribute, and reproduce various forms of digital media; and the value of those licenses are greatly diminished, to the extent that such works are made available illegally online.

With this in mind, DiMA was initially very pleased to learn of the committee's plan to focus its attention this year on foreign 'rogue' websites that are committed to massive online infringement. The congressional record is replete with ample evidence indicating that such sites pose a substantial problem for the entertainment industry, as well as software developers, apparel manufacturers and other U.S.-based IP industries. Unfortunately, H.R. 3261 does not specifically address these easily-identifiable bad actors in a meaningful way.

Instead the legislation seeks to advance an overly broad definition of an "Internet site that is dedicated to theft of US property", a definition that is filled with more than half a dozen vague new terms. The inherent problems associated with this approach have been

widely discussed by several critics of H.R. 3261, so we will not take the time to revisit those arguments in the following set of comments. However, we will focus the remainder of our remarks on one especially troubling aspect of the bill's new definition.

Section103(a)(1)(B)(ii)(I) of the legislation, in particular, seeks to rewrite a bedrock principle of U.S. copyright law by attempting to impose secondary liability on a domestic website operator based solely on their 'constructive knowledge' of infringing behavior carried out by one or more of its users.[1] Imposing liability based on this one element, without also requiring a greater showing of more direct involvement with the specific act of infringement, represents a dramatic change in existing copyright law and many subsequent judicial affirmations of the principle. This proposed change not only threatens to stifle innovation, but will likely harm consumers, unduly burden website operators and lead to an actual increase in the online infringement of digital music, movies and books.

In *Sony Corp. of America v. Universal City Studios, Inc.*[2], a seminal case in this area, the Supreme Court cautioned against placing too great of an emphasis on the element of 'constructive knowledge' when attempting to impose secondary liability on product manufacturers or service providers for infringing behavior carried out by one of their third-party users.[3] Indeed, while assessing Sony's level of liability with regard to their introduction of the Betamax videotape recorder, the Supreme Court embraced the district court's findings which assumed that Sony had constructive knowledge of the probability that the Betamax machine would be used by third-parties to engage in some minor amount of infringing activity.[4] However, relying on the staple article of commerce doctrine, the Court went on to note that holding manufacturers secondarily liable under such circumstances would unduly hamper commerce in unrelated areas and essentially deprive the American public of their ability to use the Betamax recorder to carry-out their non-infringing purposes.[5] The Supreme Court deemed such a remedy to be "extremely harsh".[6]

In addition to harming consumers, imposing secondary liability on domestic website operators under these circumstances would essentially shift the burden of policing the Internet for acts of copyright infringement from copyright owners and place the responsibility on website operators. In theory, such a restructuring may appear attractive. In practice, the policy is filled with several shortcomings.

---

[1] Section103(a)(1)(B)(ii)(I), as currently drafted, does not include the 'primary design' requirement as outlined in section 103(a)(1)(B)(i) of the legislation. Therefore, under this provision, a domestic website operator could be held secondarily liable for 'constructive knowledge' of as few as two acts of online infringement carried out by one of its users.

[2] 464 U.S. 417 (1984).

[3] The Supreme Court's decision in Sony only addressed product manufacturers, but the Court's reasoning has been extended to cover service providers, as well. *See*, In re: Aimster Copyright Litigation. 334 F. 3d 643, 648-650 (2003).

[4] Id at 426-428.

[5] Id.

[6] Id at 444.

First and foremost, copyright owners are better positioned than website operators to make initial determinations as to whether a particular use of a copyrighted work constitutes a fair use. As the 'original creator' or 'contractual owner' of a particular work in question, private rightsholders will have great knowledge of the breadth of the work in its entirety; and will be able to quickly evaluate the 'portion of the [used] work in relation to the copyrighted work as a whole' and the 'effect of [its] use upon the potential market for' the copyrighted work. As you know, these are two key elements in evaluating plausible claims of fair use.

In addition, copyright owners are better positioned to determine what licensing arrangements, if any, have been made with respect to a particular copyrighted work; and whether use of a particular work has been authorized through a third-party representative for promotional purposes. Over the course of the past few years, several news stories have been reported revealing the frequent authorized leaking of sound recordings by record companies, artist managers – and in some instances the artist himself – with the hopes of generating pre-release album 'buzz'. In light of such activities, it seems particularly inefficient to task domestic website operators with the responsibility of detecting the "*unauthorized*" release or use of such materials. (emphasis added)

Finally, it's worth noting that requiring legitimate online distributors of digital media to implement new monitoring and filtering technologies comes at a real cost. Not only in terms of the costs associated with the implementation of new protocols and systems, but also costs in terms of imposing additional expenses on an industry that already operates under rather small transactional profit margins. Ultimately, the result of this new policy will only discourage future entrepreneurs from entering into the industry and lead to a likely decrease in the utilization of the types of services offered by DiMA members which have been shown to reduce online infringement.[7]

In closing, DiMA, and its member companies, stand ready and committed to support a targeted approach to ending online copyright infringement. Unfortunately, H.R. 3261, the Stop Online Piracy Act, in its effort to rewrite a substantial portion of copyright law, fails to satisfy this standard. It is for this reason that we write to oppose the legislation, as it is presently drafted.

We welcome, of course, the opportunity to discuss our concerns regarding the legislation with committee members and staff, with a view towards crafting a new bill that more appropriately addresses the issues that face content owners and legitimate online content providers, alike.

---

[7] *See*, Alexandra Topping, *Collapse in illegal sharing and boom in streaming brings music to executives' ears*, Jul. 12, 2009, available at http://www.guardian.co.uk/music/2009/jul/12/music-industry-illegal-downloading-streaming. *See*, generally Chapter 4 of the Hargreaves Report – Copyright Licensing: A Moment of Opportunity, available at http://www.ipo.gov.uk/ipreview.htm?intcmp=239. Also, *see*, *The State of Music Online: Ten Years After Napster*, Pew Internet & American Life Project, p. 4, (June 2009).

Before the
Committee On The Judiciary
U.S. House of Representatives

Hearing on H.R. 3261, the "Stop Online Piracy Act"

Statement of the
Consumer Electronics Association
November 16, 2011

Chairman Smith, Ranking Member Conyers and Members of the Committee, on behalf of the Consumer Electronics Association (CEA), thank you for the opportunity to submit written testimony concerning H.R. 3261, the "Stop Online Piracy Act."

CEA is the preeminent trade association promoting growth in the consumer electronics industry. CEA members include product and component manufacturers, internet providers and both small and large retailers. Our industry accounts for more than $165 billion in annual domestic sales and directly employs approximately 1.9 million United States workers.

There is no doubt: CEA supports strong intellectual property enforcement. Our members' businesses rely on robust and balanced intellectual property law that protects the rights of authors and inventors while preserving and encouraging innovation, free expression and competition. As such, CEA supports this Committee's intention and determination to stop online piracy and counterfeiting. But our member companies have expressed profound concerns about the scope, sweep and efficacy of H.R. 3261, the "Stop Online Piracy Act." CEA also shares the concerns regarding this legislation expressed by innovators,[1] entrepreneurs,[2] artists,[3] and experts in law and international relations.[4]

CEA and its members are eager to support legislation that is directed to foreign "rogue sites" – the "worst of the worst" – whose infringing activities lie beyond the reach of existing U.S. authority, and have no conceivable justification under U.S. law. But as written, H.R. 3261 will do little to stop piracy and instead will undermine both bona fide online U.S. businesses, create new private causes of action and weaken the open Internet that encourages free expression.

H.R. 3261 Will Terminate Vital Financial Resources To Legitimate U.S. Businesses

Despite claims to the contrary, Section 103 of H.R. 3261 empowers private parties to require payment processors and Internet advertising services to suspend all services to entire web sites of legitimate U.S. businesses and not just foreign rogue websites. This death sentence to an entire legitimate U.S. business can be triggered by a single complaint from another company simply claiming that a copyright infringement or a violation of Section 1201 of the DMCA is

[1] *See, e.g.*, letter to this Committee from Internet engineers, October 12, 2011.
[2] *See, e.g.*, open letter to Chris Dodd from Masnick *et al.* Silicon Valley entrepreneurs, October 31, 2011.
[3] *See, e.g.*, letter to Members of Congress from 96 law professors, July 5, 2011.
[4] *See, e.g.*, open letter from artists to Members of Congress from Fight For The Future, October 14, 2011.

being "enabled" or "facilitated" or that the business failed to take advance measures to cleanse itself of every product against which some complaint ***might*** be brought.

H.R. 3261's **extremely** overbroad definition in Section 103 of "dedicated to theft of U.S. property" endangers innovation and legitimate commerce. Despite the use of terms such as "U.S.-directed," this section is not limited to overseas sites. It targets and affects all U.S. sites and all U.S. businesses. Businesses said to be only "enabling or facilitating" infringing conduct by other domestic or foreign companies will face a risk of being shut down that is equal to those actually "engaging" in it. Applying this broad standard to copyright infringement and to Section 1201 of the DMCA, and allowing *anyone* to demand that access to payment providers and Internet advertising be denied, opens the door for mischief on a scale not seen in even the most dubious copyright and patent litigation. For example:

- A website offering a legitimate but controversial product could be shut down entirely by a notice from a private plaintiff to a financial transaction provider, or to an advertising service. The law would require not just a "take down" of the controversial product, but a ***shutdown*** of all online purchasing and advertising for ***any other*** product on the site. The plaintiff need only complain that the business is "marketing" a product for a "use" that would be copyright infringement.

    - This sort of claim has been commonly, and often unsuccessfully, made against innovative and legitimate consumer electronics products. In 2000, such a claim was made by several motion picture studios against Replay TV, an early competitor of TiVo and a forerunner of the DVR products now routinely distributed by cable and satellite companies to their subscribers – based *only* on the product's ability to search, record, index, and retrieve content.[5]

Such a "market-based" private action under Section 103 of H.R. 3261 would be a chilling alternative to filing a copyright suit for contributory infringement or inducement – the sort of suit that Sony *won* in the Supreme Court when the first VCR was challenged. It would be necessary only to persuade credit card issuers that a complaint of contributory infringement or inducement is "reasonable" – instead of prevailing in an adversarial court proceeding. Due process is dealt another blow in the legislation since Section 103(d)(5)(B) immunizes credit card issuers from liability for acts relating to or "reasonably designed" to comply with a private request to shut down all payment processing for all the challenged company's online products.

Because Section 103 also covers "enabling or facilitating" a violation of Section 1201 of the DMCA, private actors could also ask credit card issuers to shut off payments to any site that offers a product that they accuse of "circumvention" under the DMCA. But companies have suffered losses from preliminary injunctions based on improper "circumvention" claims, as the courts have struggled with the open-ended language of Section 1201 of the DMCA. By broadening the scope further to include acts of "facilitation" under a law in which marketing and

[5] While competing and successor products offering the same capacities have thrived, Replay sold off its assets in bankruptcy because it could not fund its defense of the lawsuits. Some of the complaints filed against Replay claimed that the ability to search for, record, and index content from cable TV, taken alone, constituted direct, contributory, and inducing infringement of copyright.

facilitation are *already* punishable and immunizing banks that shut off funds to those accused can only further chill technical innovation and legitimate commerce.

Per Section 103(a)(1)(B)(ii)(I), companies accused by private sector rivals or other private actors of "enabling or facilitating" violations of copyright law or DMCA 1201 are *also* vulnerable to a charge of having taken "deliberate actions to *avoid confirming* a high probability of the use of the U.S.-directed site to carry out acts that constitute a violation ...."[6] In plainer language, this would seem to suggest that domestic online merchants offering thousands or tens of thousands of products in their online stores will now be required to *police* their listings in advance for possible claims of copyright "inducement" or direct infringement. This provision would also seem to eviscerate the protections for online services, search engines, and consumer participation Internet sites offered by DMCA Section 512.[7] CEA believes that legitimate U.S. merchants and Internet companies should not be responsible for advance *economic cleansing* of their sites to avoid lawsuits. If this provision is enacted, innovators and other legitimate business could not even rely on the discretion of federal prosecutors. Instead, they would be at the mercy of litigation-happy companies that want to preserve aging business models or shut down competitors.

H.R. 3261 Would Shut Down Legitimate U.S. Websites Without Due Process or Recourse for the Wrongfully Targeted Website

Under Section 104, the legislation provides complete immunity for a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name register from blocking access or financial services to a website so long as there is a "reasonable" belief that the site is "dedicated to the theft of U.S. property."

There is no due process for the innocent website owner to defend themselves before the action is taken or seek restitution after their website has been removed and business negatively impacted.

With the threat of being sued for contributory infringement coupled with the broad definition of "dedicated to the theft of U.S. property, a service provider will have a strong incentive to shut down the accused website. To put it simply, the legislation favors the copyright owner's intellectual property rights and, based on unfounded claims of infringement, strips the accused website owners from their property right.

---

[6] Section 103(a)(1)(B)(ii)(I), emphasis supplied. As is noted above, despite use of terms "U.S.-directed," etc., the businesses targeted and affected by Section 103 include all U.S. Internet sites and all U.S. businesses.

[7] Counsel for content providers have criticized court implementation of this "safe harbor provision," which was painstakingly negotiated with congressional leaders and the tech industry as a core part of the DMCA. *See* Greg Sandoval, RIAA lawyer says DMCA may need overhaul, Nov. 6, 2011, http://news.cnet.com/8301-31001_3-57319344-261/riaa-lawyer-says-dmca-may-need-overhaul/?tag=mncol;posts.

H.R. 3261 Creates Security Risks that Outweigh Potential Blocking of Illegal Sites

H.R. 3261 also includes a "DNS" blocking provision that is more dangerous to legitimate business than it is to pirates. The DNS blocking provision also invites similar action by nations that are not as scrupulous about free speech and an open Internet as is the United States.

It is easier for a "pirate" site to circumvent DNS blocking than it is for a legitimate business. A "pirate" expects to be pursued and is ready to use other names that can easily be found by those accustomed to actively searching for such sites. Legitimate businesses, however, invest in their brands and attract customers who look for the brand. Thus, improvident or mistaken use of the name blocking technique – shown already to be inevitable by those operating in the best of faith – will hurt innovative and legitimate businesses more than it will pirates.

When foreign governments point to this law in order to rationalize new uses of DNS blocking to suppress internal speech or the competition from U.S. and other legitimate businesses, our innovation, as well as our society's interest in free speech and an open Internet, will suffer.

* * *

CEA concurs with the other issues with H.R. 3261 raised by NetCoalition, Public Knowledge, the library and educational associations, and the many innovative technology companies that have expressed concern over its potential impact on their legitimate business practices. Their concerns and ours, along with those voiced by experts in several other fields, should lead to a deliberate examination and a narrowed focus of this legislation. On behalf of our members, CEA pledges its cooperation and its assistance in this process.

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

The White House

Office of the Vice President

For Immediate Release
November 01, 2011

VP's Remarks to London Cyberspace Conference

Via Video Teleconference

10:42 A.M. EDT

THE VICE PRESIDENT: Well, thank you very much, Foreign Secretary Hague, and my best to Prime Minister Cameron. I agree with everything that he said today.

But I'm very glad to be able to join you all on behalf of our administration to talk about the issue that will have enormous, enormous consequences for each of our countries and, quite frankly, consequences for the whole world: the future of cyberspace.

And I do bring greetings from Secretary Clinton who does send her regrets that she's not able to be with you in person today.

As you all know, nearly one-third of humankind is online today, something we would have never thought possible 20 years ago, more than 2 billion people and counting. The Internet has become the public space of the 21st century, a sphere of activity for all kinds of activities, open to all people of all backgrounds and all beliefs.

And as vibrant, as dynamic as the Internet already is what we've seen so far, I believe and we believe, is just an opening act. More than 5 billion people will connect to the Internet in the next 20 years -- 5 billion. And most of them will live in countries and regions that are now under-represented online. And the next generation of Internet users has the potential to transform cyberspace in ways we can only imagine. And cyberspace, in turn, has the potential to transform their lives, as well.

But the extent of both the contributions they will make to the Internet and the benefits they'll derive from it are going to depend in large degree on the choices all of us in the room today make. The Internet itself is not inherently -- to state the obvious -- is not inherently a force for democracy or oppression, for war or for peace. Like any public square or any platform for commerce, the Internet is neutral. But what we do there isn't neutral. It's up to us to decide whether and how we will protect it against the dangers that can occur in cyberspace while maintaining the conditions that give rise to its many benefits. That's what Prime Minister Cameron just spoke about.

And today I'd like to explain briefly where the United States stands on key issues regarding the future of cyberspace. First, which approach should we take for ensuring that Internet -- that the Internet itself continues to be secure, open to innovation and interoperable the world over; secure enough to earn the trust of our people, and reliable enough to support their work?

And secondly, how do we achieve security for nations, businesses and people online without compromising the openness that is the Internet's greatest attribute?

It seems to us that answering these questions is a key priority for not only our administration, but for all of you assembled in the room; and to articulate our position, we laid out the International Strategy for Cyberspace.

We know that it will take many years and patient and persistent engagement with people around the world to build a consensus around cyberspace, but there are no shortcuts because what citizens do online should not, as some have suggested, be decreed solely by groups of governments making decisions for them somewhere on high. No citizen of any country should be subject to a repressive global code when they send an email or post a comment to a news article. They should not be prevented from sharing their innovations with global consumers simply because they live across a national frontier. That's not how the Internet should ever work in our view -- not if we want it to remain the space where economic, political and social exchanges can flourish.

Now, there are some who have a different view, as you all know. They seek an international legal instrument that would lead to exclusive government control over Internet resources, institutions and content and national barriers on the free flow of information online. But this, in our view, would lead to a fragmented Internet, one that does not connect people but divides them; a stagnant cyberspace, not an innovative one, and ultimately a less secure cyberspace with less trust among nations.

So the United States stands behind the current approach which harnesses the best of governments and private sector and civil society to manage the technical evolution of the Internet in real time. This public-private collaboration has kept the Internet up and running all over the world.

We have an expression in our country: If it ain't broke, don't fix it. It would be misguided, in our view, to break with the system that has worked so well for so long. However, as the Prime Minister pointed out, there are ways we can improve on what we're doing; for example, by bringing greater transparency and accountability to Internet governance and institutions, by including more voices from developing countries and by supporting successful initiatives like the Internet Governance Forum.

Just as important in our view, as to whether the Internet functions effectively, is what people are free to do there in that space without fear of being targeted by criminals or having their private information exposed or being punished by their governments for expressing their views online.

And this brings me to the second question that I'd like to address today, how to achieve both security and openness in cyberspace. As we all know, the openness that makes the Internet a

---

Mr. ISSA. Thank you, Mr. Chairman. I have been the victim of piracy, so you are not going to have a problem with me agreeing with the problem. Hardware/software, got it all. But, Mr. Clark, I am going to hope that you can stretch for this part of it, even though it is not in your title. You are familiar with the ITC, are you not?

Mr. CLARK. Yes, I am.

Mr. ISSA. Pfizer regularly for patent infringement on imported products would go to the ITC and get relatively quick justice using

administrative law judges available to them, injunctive relief against a patent violator, correct?

Mr. CLARK. Outside of my field, but I would believe that would be the case.

Mr. ISSA. So, when we deal with rogue elements outside the jurisdiction of the United States that are importing in the United States, we have a history of an organization that is quick, administrative, and can have continued jurisdiction against non-U.S. entities who are, in fact, trying to take what they have stolen and sell it into America. Is that correct to your understanding?

Mr. CLARK. Generally speaking, yes.

Mr. ISSA. Okay. Have any of you—just raise your hand—worked with the ITC in your background or are familiar with them? One or the other.

Well, let me just run through quickly, because time will be very limited and the answers seem to be long. We have a court of jurisdiction. Now, they do not specifically have the mandate to follow the money and provide injunctive relief against Google, eBay, or anybody else after they find an offshore infringer and seek remedies, but they have their own counsels. They have administrative law judges. They have a procedure.

Mr. Chairman, I object to this bill in its current form, mostly because I believe it fails to use tools that are generally better than the tools that we have at our disposal in this bill. And I believe that if the real remedies sought is, in fact, a court of continued jurisdiction specializing in intellectual property and designed to it, in fact, reach a quick solution to a question of whether there is wrongdoing, and then follow the money through injunction, not through fines, and obviously a criminal referral.

My intention is to offer legislation on a bipartisan basis that will, in fact, look at the legitimate concerns, take a great deal of these 80 pages; however, and this is where it is tough, Mr. Chairman and Ranking Member, suggest that a jurisdiction not within this Committee get a substantial portion of this bill, because I believe that that is as appropriate as it is for the Federal courts to consider domestic entities who are violating it.

And so, with that, Ms. Oyama, if I am pronouncing it right.

Ms. OYAMA. Yes.

Mr. ISSA. In your experience, has Google worked with the ITC or any other administrative law judges and executing on other people's judgments?

Ms. OYAMA. I would imagine in the patent context, yes. It is not my field, so I cannot speak to it.

Mr. ISSA. Okay. But do you agree that having a court of continued jurisdiction that, in fact, can work for injunctive relief as technology is available is generally something that Google and the other search engines would see as reasonable once there is a judgment entered against an offender somewhere?

Ms. OYAMA. Yeah, I think we would be happy to work on that type of solution.

Mr. ISSA. And I am going to get to the others, but, Mr. Clark, if you had that, and you had a judgment against party A who had an Internet site, and then 25 other similar parties show up from the same country and have all the identities that tell you it is basi-

cally the same group of you already have a judgment against, would you not benefit from a court that we specifically gave jurisdiction to to determine quickly that those are alter egos and execute upon them so that you would not go through this wackomo again and again, trying to prove to somebody that it is basically the same people doing it again?

Mr. CLARK. My working relationship with the ITC has been very, very limited. I am not quite certain what their capabilities are. If you are saying you are going to empower them to do certain work like that, it would make some sense.

Mr. ISSA. Currently they are, and the others would probably know this, it is a place that plaintiffs go to if there is any importation and they have a patent because they can administer a decision faster than the fastest rocket docket. And unlike the eBay decision, they have injunctive relief, not only as a tool, but as their one and only tool, and they use it without discretion because, in fact, that is the mandate of Congress.

Mr. CLARK. But you are still talking of a referral process. I think the DoJ then for a criminal follow-up and for asset——

Mr. ISSA. And I recognize at some point the administrative law judges look and say we have a domestic entity that is not compliant with our injunctions, or a site that is just as broke in the U.S. So, I am very aware that there are elements here that if you are cooperating or facilitating with a foreign entity, that there would have to be a referral. That is not going to be Yahoo, or Google, or eBay. It is going to be, as you know, the rogue sites you fight every day.

Mr. CLARK. Right. And I would just be worried about the bifurcation of activity in the referral process and the elongation of the end result is something like that were arranged.

Mr. ISSA. Well, I look forward to showing both our witnesses and the Committee that, in fact, the ITC's time to judgment and their execution is actually much shorter than our Federal courts, and less discretionary than the Justice Department's generally. And I thank the Chairman for his indulgence, and yield back.

Mr. SMITH. Thank you, Mr. Issa.

The gentlewoman from Texas, Ms. Jackson Lee, is recognized?

Ms. JACKSON LEE. Let me thank the Chairman very much, and the Ranking Member, and let me call the roll, for the record, and say that I want the U.S. Library of Congress, I want Pfizer, the Motion Picture Association of America, MasterCard, Google, and our good friends in the technical aspect of our moviemaking business, and all supporters to be made whole. I think we have a consensus that online piracy is a both devastating and destructive element of the Nation's economy. In fact, I have said, I think, I believe often that it steals the genius of this country.

We are very proud of the motion picture industry, and I am, if you will, a cup runneth over. I may be your physical armor when I see the massive thievery that goes on, and certainly in some of our international friends.

So, I start off with that, and I want to find a common ground. And as I have looked at the legislation, I hope the Chairman and Ranking Member will give us the time to really study the legislation. Several things come to mind. One, this legislation has no re-

ferral. I am a Member of the Homeland Security Committee, and our Committee spent years helping to build the switch to the DNS-SEC. And if this bill would pass, we would have a challenge with that format.

And the question is, would everyone who needs to make changes to the DNS-SEC would instead be on the phone to their lawyers, asking whether they would be sued for adopting security technology that will make the mandated block and redirect system even more difficult. We have to look at all of these issues.

So, I want to ask the Library of Congress first if she has any comments regarding that conflict. We are supposed to be collaborative. You are the only government witness. I am not sure if you have thought of that, but let me give you a second question quickly since our time is going quickly. I am concerned about what effect it will have on small businesses, particularly those that could not afford to go to court should a rightsholder come forward and demand that their access to revenue be shut off. If a rightsholder accuses a small business website of facilitating infringement and a payment processor shuts off payments to that business, is the payment processor immune from suit under section 104, and what rights do they have?

So, first, is there any collaboration or recognition about the system that the DHS has formulated?

Ms. PALLANTE. I am sorry, I do not know the answer.

Ms. JACKSON LEE. You do not have that question. Mr. Chairman, I think we have to have that answer from whatever resources we can get.

Next, if you can have any insight on how it impacts small businesses——

Ms. PALLANTE. Yes.

Ms. JACKSON LEE [continuing]. This particular legislation.

Ms. PALLANTE. That section of the bill, I believe, was actually intended to make it easier and quicker, and to avoid the court process and the cost. That is the goal. There is no liability for the intermediaries under that section. There is an obligation if it goes to the next stage and there is a court order. There is an obligation.

Ms. JACKSON LEE. Right. So, there is still a process that is small business might have to be engaged in. There is still a process which makes it easier——

Ms. PALLANTE. There is, and they are good faith intermediaries, and they have not themselves broken the law, and the bill tries to take that into account. If we can refine that, we should.

Ms. JACKSON LEE. Yes, because they still have an obstacle to climb, if you might.

Let me go to Ms. Oyama. Forgive us all for not reading the name correctly. I do not have it in front of me. But let me quickly give you a series of questions.

Ms. Oyama, is that correct?

Ms. OYAMA. Yes.

Ms. JACKSON LEE. All right, thank you. One of the kinds of groups that I have been engaged in over the last couple of months is the generation of youth that are excited about startups. They are everywhere. They are job creators, and I see them as the next nucleus of job creation in America. They are obviously functioning

now. They are all trying to emulate all of the stars of social networks. We know that will not be the case, but they are trying to create jobs.

So, let me raise these concerns with you. I think immediately what comes to mind is that this legislation may be overly broad, that it too easily circumvents Internet users, and it is inherently incompatible with the way the Internet actually works. Would you comment on the overbroad, these circumventing Internet users, and incompatible with the way the Internet works? Could you do that quickly for me? And then, I would like to go back to—if you could be listening to this question about the—Ms. Pallante, if you have any idea about the problematic aspect of this, again, for smaller minority businesses. But, Ms. Oyama?

Ms. OYAMA. Sure. On the over breadth concern——

Ms. JACKSON LEE. Over broad.

Ms. OYAMA. Over broad, a huge concern is the scope of the definition of what is a site dedicated to the theft. So, that is a concern that has been raised amongst small businesses, larger tech companies. If we are going to go after rogue sites, we have to make sure that they are rogue sights and they are breaking the law. There is a lot of concern that right now. The definition would cover new ground. It would cover sites that today are complying with the DMCA, so they are taking down infringement when they are notified by rightsholders. It would be sites that today under existing laws if they were hauled into court, they would be found not guilty under existing copyright laws. So, I think there is the scope concerns there.

Ms. JACKSON LEE. Circumvented by Internet users? It could be too easily circumvented by Internet users?

Ms. OYAMA. Yeah. So, one of the concerns is that on the notice and terminate provision, that peace does not go through the courts, and so somebody could just notify a service provider. You could go away for Thanksgiving if you are a website owner, and your ads and payment providing services under the bill should be could be shut off in 5 days. So, there is a lot of concern that, you know, that does not really provide adequate due process in terms of the way current businesses work.

I will say in terms of the incompatibility with the Internet, in the Internet sphere, Internet traffic is going to route around blockages, and so kind of working with a grain of the Internet we think is really smart, is really effective. It is why we support the legislation. We have discussed before about cutting of the funding sources. It is an incredibly sophisticated site. Much of international law enforcement was going after Wikileaks, and if you go to Wikileaks home page, it says that they are going down because payment providers shut them off.

Mr. SMITH. The gentlewoman's time has expired.

The gentleman from Florida, Mr. Ross, is recognized?

Mr. ROSS. Thank you, Mr. Chairman.

Ms. Oyama, do you feel that this bill is an infringement of the First Amendment right of free speech?

Ms. OYAMA. You know, I think short of the constitutionality; it certainly raises free speech concerns.

Mr. ROSS. Is it censorship that you are concerned about?

Ms. OYAMA. Yeah. So, the U.S. has had a good platform globally to speak out for free expression, and I think a lot like this, which would for the first time empower the government——

Mr. ROSS. It would empower the government to require you to do something that you do not want to do, which would be to shut down a site. Is that correct?

Ms. OYAMA. We are happy to disable links, when we are notified by rightsholders. We think that——

Mr. ROSS. And as long as you do it without a third party, such as the government, it is not an infringement of First Amendment rights of free speech, nor is it a censorship, is it?

Ms. OYAMA. We do not do full site blockages; we do page by page for a——

Mr. ROSS. But you do takedowns.

Ms. OYAMA. Under DMCA, yes.

Mr. ROSS. Yes, which is the same thing. I am just having a hard time distinguishing when you do it. It is okay, but when you have the third party, such as the Federal Government, requiring you to do it, then it becomes censorship and an infringement of First Amendment rights.

Ms. OYAMA. I see. I think the government approach is much broader in this bill.

Mr. ROSS. Let me go a little further here because I want to go your example of Dave's Emporium, which I think is a great example for people, such as me, that think simply to understand a small business. But I want to look at it from a consumer rights perspective.

Let us say that Dave's Emporium, because of that 1 percent vendor that he uses on the Internet that is found through your Google search, results in the purchase of a product that causes death or personal injury. Now, in that chain of commerce, Google would be brought into action, especially where there is joint and several liability as a deep pocket, to defend that suit and probably pay damages. All of that could have been prevented had there been an investigation, had there been the appropriate execution under this Act.

In fact, not only would it have been prevented, but also under this bill, is there not an affirmative defense that Dave's Emporium could have asserted in the sense that I do not have the resources to hire a lawyer that would mitigate my responsibility to now have to defend the order to take down.

So, what I am getting is that, even further you have immunities under this Act that would prevent a third party suit against you if you shut it down. But you do not have immunities if, in fact, you allow for the sale and purchase of products that are not only counterfeit, but they also result in death or personal injury.

Ms. OYAMA. So, on counterfeit, it is definitely something that we agree with you. Counterfeit is a big problem. It is something that we invest tons of engineering hours, millions of dollars, into going after. For example, for ad words, we ejected 95 percent——

Mr. ROSS. But it would seem to me that you would want to have the immunities. You would want to have some protection, some safe harbors to prevent lawsuits against you in the execution of your business.

Ms. OYAMA. I think if a court is instructing intermediaries to take action, there is probably some plays for its immunities. But the concern here is that Dave could be shut off for 5 days, not pursuant to his terms of service. Certainly no one has an absolute——

Mr. ROSS. But he could be put out of business being sued because of the harmful product that could have been prevented had Google investigated the site.

Ms. OYAMA. So, certainly, no one has an absolute right to ad payment services. We think that there should be——

Mr. ROSS. Well, Dave is in a bad situation either way, and I think that he needs to have some protections, and I think that this bill will offer some of that.

But let me shift to another thing, and let me tell you, I appreciate what Google has done with regard to child pornography. I mean, you guys have stepped up to the plate tremendously. And I think that is a wonderful example; you need to be congratulated for that. You do it because it is the right thing to do. And it would seem to me that following the letter of the law, you could do the same thing in this regard in an effort to hold down or at least eliminate the use of pirated sites by way of the search engine, Google.

Ms. OYAMA. So, child pornography certainly is a huge problem. It is something we take very seriously. Technically, going after child pornography in a search engine is completely different from copyright because a machine can detect tapped child pornography, and a machine can look for flesh tones. Human, if you look at it, would know what it is and could ejected, and with a copyright——

Mr. ROSS. But it is still the right thing to do.

Ms. OYAMA [continuing]. You cannot just look at the video and know whether it is infringing or licensed, right? It needs to be in collaboration with the rights owner.

Mr. ROSS. Real quickly, Ms. Kirkpatrick, not a question, just a thank you on behalf of MasterCard for what you are doing because you are cutting off the source of the problem. And that is very important.

Ms. KIRKPATRICK. Thank you.

Mr. ROSS. Mr. Almeida, I had a chance to meet a couple of days ago with one of your members, a gentleman, a lifelong songwriter. He is in this room. And he met with me, and he said, you know, the problem is not that it is a fight between the movie houses and the producers; it is the small people, the people who have followed their passion, the people who have the artistic ability to do something they have always wanted to do that now, after 30 years of being a songwriter has to look at whether he can keep his house, what his future is going to hold. And I wish you would do for me, and explain to the Members up here, is how this adversely impacts not the giants in Hollywood, and not the giants in Nashville, but those that participate, those whose creativity and innovation will be stifled unless there are some protections.

Mr. ALMEIDA. Well, I think there does need to be protections, and I think that is what this bill hopes to do. And this is not to protect the big dogs in Hollywood.

Mr. ROSS. Right.

Mr. ALMEIDA. Our members who are behind the scenes, who are stage hands——

Mr. ROSS. The foundation.

Mr. ALMEIDA [continuing]. The people who build the sets, the back end payments for those workers support their health and pension fund, and that is being cut off. They are adversely being impacted by these rogue site sand by the piracy of their videos. A video being released today will be available by the weekend on the web. And so, we are hoping that this legislation will help to take a step forward in that area.

Mr. ROSS. Thank you. I see my time has expired. I yield back.

Mr. SMITH. Thank you, Mr. Ross.

The gentlewoman from California, Ms. Waters, is recognized?

Ms. WATERS. Thank you very much, Mr. Chairman.

Let me just say that I find the discussion on H.R. 3261 extremely interesting and engaging. I think Mr. Watt framed this issue somewhat in his opening statement when he talked about the giants, and competition, and the profits and the money that is involved being at the basis of all of it. And let me just say that I view any proposed changes in IP and copyright law as an opportunity to examine whether changes will expand opportunities for women and minority entrepreneurs, both in Hollywood and Silicon Valley.

And I come to this discussion just having witnessed a CNN presentation called "Black in America" by Soledad O'Brien this past weekend, which I found very, very interesting.

Having said that, I would like to direct my first question to Maria Pallante, U.S. Copyright Registrar. User generated content, websites like Facebook and YouTube, are extremely popular. Individuals and groups use these platforms to share videos that range from fraternity and sorority step shows and high school talent shows, to videos of kids performing a new dance or imitating a new music video. Many of the common artists who do not have record deals also use UGC sites to showcase their talents, covering popular songs.

Now, to the extent many uploaded video clips feature the use of copyrighted music and other type of content that is not for profit or commercial gain, do you think that this bill would include a safe harbor, their use exception or other explicit provision that would ensure we are not trying to subject parity and leisurely activities to felony penalties? Are you at all concerned that some of the section's broader language could have unintended consequences that may chill the use of UGC sites and digital platforms that have served an important source of social utility?

Ms. PALLANTE. Thank you for the question. I am not concerned as it is written. We are talking about two different levels of activity. This bill would go after sites dedicated to infringement. I think what is on the table in this room is a position that one can be compliant with the DMCA through notice and takedown of very specific sites when notified, and, therefore, not have an obligation to participate in a solution that is about fraud, willful, criminal, egregious, dedicated activity. These two things will operate at the same time, and the notice and takedown system will remain intact.

Ms. WATERS. Also I would like to ask about another issue that I am very concerned with, and I would like to direct this to Ms.

Katherine Oyama, to Google. I am very concerned about the voluntary authority and legal immunity the bill gives Internet service providers to block access to sites they reasonably believe are infringing sites. This provision would seem to run counter to the FCC's recently issued open Internet net neutrality rules.

I can foresee cases in which an Internet service provider that owns online content may use this section as pretext to unfairly block access to a competing website that is not really dedicated to infringement. This section does not require credible claims, merely a reasonable belief that does not exclude commercial disputes or anti-competitive conduct. It is my understanding that the Senate does not have ISP involuntary blocking authority in its bill.

Can you foresee any unintended consequences with the voluntary blocking provisions? Is there a way that this bill could be refined to ensure that voluntary actions are based on credible evidence and certain thresholds?

Ms. OYAMA. Sure, thank you. So we do see today, the Internet used by countless small businesses to facilitate communication to facilitate e-commerce. It is truly people's daily livelihood, and so we do think there should be due process built-in if something essential to your site, like your services, is going to be taken away.

I think the provision you are mentioning is Section 104 in the bill. I think the broader technology community shares those concerns. You know, want, if you look at the scope of sites that could be captured by a service provider's reasonable belief that they were dedicated to theft within the bill, that is a very broad group. And then, two, the number of service providers that receive complete immunity for terminating service without going through a court, without going through due process. It is not just the providers that are required to take action under this bill; it is much broader. So, it would include advertisers, search engines, payment providers, but also domain name registers, ISPs, you know, a much broader group of folks.

If you were to lose your domain name and you are a small and independent business, that is everything. And so, making sure that you are at least protected by the terms of service when you sign up for the contract would, you know, probably makes sense to us.

Ms. WATERS. Thank you very much, Mr. Chairman. I yield back the balance.

Mr. SMITH. Thank you, Ms. Waters.

The gentleman from Iowa, Mr. King, is recognized?

Mr. KING. Thank you, Mr. Chairman. I appreciate being recognized, and I appreciate the testimony of the witnesses.

I wanted just to take a bit of a different tack here, if I could, and looking at the fraudulent Internet sites and the peace of this that is a direct focus of this hearing. And I am just looking through some of the background material, the problem of illegal pirating of copyrighted intellectual property. And I would think that it is all trademarks, and copyrights, and patents all together that I think about, not just websites and things that we can look at.

And so, there is a pattern across this country or across the world of certain countries that are pretty effective with this. And I just ask if there is anybody on the panel, just raise your hand, or answer. Do you have a list of countries that are the most egregious

violators of intellectual property rights from an American perspective? Yes, sir. I cannot read your names, I am sorry.

Mr. O'LEARY. Thank you, Congressman. It is Michael O'Leary.

The content industries contribute to something through the State Department. There are a number of different ways. There is a notorious markets filing, which chronicles the areas of the world where this is the most problematic, and then there is a special 301 process whereby the United States puts forward a list and kind of categorizes where countries fall in terms of their protection of intellectual property.

And the reason for that, frankly, very simply, is that intellectual property is not just an American problem; it is a global problem. And what you are seeing around the world is that other countries are starting to recognize the benefit of not just protecting American intellectual property, but protecting their own.

I would note, for example, that there are at least 16 countries in the world that engage in sight blocking now, which has been the focus of some of the debate here. The Internet seems to be working fine in those countries. It seems to be having an impact in terms of taking sites, like the Pirate Bay, which is blocked in many other countries, but not in the United States, offline.

So, in many ways, the United States has historically been a world leader, but the truth of the matter, Congressman, from our perspective is, if we do not step up and deal with the problems we have today, we are going to cede that ground, and we are not going to be the world leader. And that is unfortunate for our country, because we do lead the world in the production of intellectual property, and we ought to be leading the world in protecting it.

Mr. KING. Mr. O'Leary, do you have an opinion then? You have given me a couple of sources I might look at. Do you have a recollection on from which countries originate the greatest theft of intellectual property?

Mr. O'LEARY. Off the top of my head, I would hesitate to list them and any type of specific order. I mean, there are different problems in different parts of the world. There are hard goods problems, which is kind of more the traditional disk type piracy that that occurs in places like Russia. There are problems with online; a country like Spain has a significant online piracy problem. There are other places in Europe.

We would be happy to provide you and the Committee with a complete list. I am hesitant to speculate because I do not trust my memory well enough to get them in the right order.

Mr. KING. Is China on your list?

Mr. O'LEARY. China is on the list, yes. There is definitely a piracy problem in China, yes.

Mr. KING. And do you have any recollection of what the loss might be to American property rightsholder from China?

Mr. O'LEARY. I do not off the top of my head. I am not sure, frankly, that there is a way to measure it given the realities of China.

Mr. KING. Would anyone on the panel be aware of any studies, U.S. Trade Representative? It seems to me that three or 4 years ago at least, a U.S. Trade Representative has a study done that calculates that loss to U.S. intellectual property rightsholders to

different nations, China and Russia come to mind. Anyone care to answer that? I saw a nod on the end of the line.

Ms. PALLANTE. Maria Pallante from the Copyright Office. I do not have the dollar amount for you, but I would just echo what Michael said, which is that the special 301 process identifies problematic standards in our trading partners when it comes to IP, as well as notorious markets and websites.

Mr. KING. Does anyone have more of a comprehensive solution? We are talking about shutting down some websites. But it is billions in theft of intellectual property rights globally. And here we are in the United States of America with some of the strongest laws and the strongest traditions and respect for intellectual property. And I do not see a broader comprehensive solution to this.

It seems to me that they can move faster than we can adjust to them, and that we are dealing with a component rather than the big picture. Yes, sir, Mr. O'Leary, and then——

Mr. O'LEARY. Congressman, I would argue that you are correct in the sense that this is a global problem. It is multi-faceted. There is not a single approach that fits. But it is critically important that the United States maintain the high ground and the leadership in this because if we do not do it, other countries will not.

I would also note that the problem you are highlighting about the criminals moving faster, that is true regardless of what the crime is. You ask anyone in law enforcement that and they will tell you, you catch the ones who keep doing the same thing, and the people who adapt and change, you have to keep changing that.

Mr. KING. Are you aware of any State-sponsored intellectual property right theft?

Mr. O'LEARY. Are we worried about it?

Mr. KING. Are you aware of State-sponsored?

Mr. O'LEARY. We believe that that occurs, yes.

Mr. KING. And I want to say, I believe that happens from China as probably the lead globally to do that. Does anyone disagree with that on the panel? I did not hear any disagreement.

I think I have gone far enough with this since my red light came on. But I do appreciate all your testimony, and I hope we can bring some peaceful solution to this. And I hope at some point we can bring a whole solution to it.

Thank you very much, and I yield back the balance of my time.

Mr. SMITH. Thank you, Mr. King.

The gentleman from Tennessee, Mr. Cohen, is recognized?

Mr. COHEN. Thank you, Mr. Chairman. This is indeed an important issue for us to work out, and the theft of intellectual property is of great concern. But nevertheless, First Amendment issues are important, too.

And my first thought is, it does not seem like that there should be that much difference from what the Google folks and the techie folks are wanting and what the MPAA and the RIA and the other AAs want.

Let me ask maybe the gentleman from motion pictures, who apparently has a Rick Perry problem with not being able to count to something, Mr. O'Leary. Have you all not gotten together and tried to work this out in some way and fine tune this to where there are not these issues of people being penalized that are not guilty and

sites being shut down where there is just a small infringement, but not a total infringement?

Mr. O'LEARY. Well, we do not believe that this legislation will result in either of those things happening. But our studios work with Google on a regular basis in terms of trying to get stuff taken down off the Internet. There are ongoing relationships.

On this piece of legislation there have not, to my knowledge, been specific discussions about this. But I want to be very clear. We have said from the beginning that if people are willing to come forward with constructive suggestions on how to do things that are not a pretext for maintaining the status quo, that we would listen to those things.

Mr. COHEN. Wonderful.

Ms. Oyama, do you have some positive, you know, not under a pretense type, pretext type of discussions that you would like to come forth with?

Ms. OYAMA. Yes. So, I think just in the broader context of figuring out how to go after piracy, it is really important to keep in mind the number one most effective tool for going after piracy would be to increase the amount of legitimate, lawful services that are available on the Internet, right? So, if we can cut off the funding, we would decrease the supply of these pirate sites. If we could have more legitimate services for music and movies and everything else, which I know the studios are working very hard to do, that would also decrease the consumer demand for this type of——

Mr. COHEN. Without itemizing each of them now, have you had the opportunity——

Ms. OYAMA. Sure.

Mr. COHEN [continuing]. Have you had the opportunity to pose these to other team?

Ms. OYAMA. Yeah. So, although we are here in D.C. today, I would assure you that all of our businesses partners, you know, on the West Coast are working very collaboratively, very, you know, much together to get to those solutions. And we are always more than happy to continue to work with Mr. O'Leary and others.

Mr. COHEN. So, are you all working now trying to come up with some language that the Chairman might put in a manager's amendment that would make all people happy?

Ms. OYAMA. You know, there has been some conversations, but I think there would need to be a lot more.

Mr. COHEN. I would hope there would be a lot more, and I think that is something that should take place.

Let me ask you a question since you are on the microphone. There are a couple of search engines in China and Russia, and Yandex I think is one of them, and Baidu. And some consider these rogue sites, and whether they are or not, I do not know. They could be.

If they were considered such and they were blocked because they had some pirate type folks among their constituency, how do you think the Chinese and Russians would respond toward your company and toward the United States' companies?

Ms. OYAMA. That is an excellent question. So, I think we should realize that even though we would do something for a really good reason here, it could potentially have international ramifications. If

the U.S. government is ordering U.S. companies to disappear foreign search engines from our results, it should be expected that there is going to be some form of retaliation internationally.

Mr. COHEN. And those sites are the leading Chinese and Russian search engines, is that correct?

Ms. OYAMA. The sites that you mentioned?

Mr. COHEN. Yes, ma'am.

Ms. OYAMA. Yeah.

Mr. COHEN. Yeah. So, is it possible under this legislation, they would be totally cut off entirely?

Ms. OYAMA. If they were deemed rogue sites——

Mr. COHEN. Right.

Ms. OYAMA [continuing]. Under Section 102, search engines could receive an order to disappear the whole site.

Mr. COHEN. Right.

Ms. OYAMA. It is really tough in a search engine because although you can remove the direct link from a search, you know, as long as a rogue site exists, people are still going to talk about it. They are still going to blog about it. They are still going to post about it. And so, it is really not possible to remove all worldwide discussion of a link. And that is why we support the follow the money type legislation because that is really going after the source of the problem by choking off their financial reason to exist.

Mr. COHEN. Let me ask you another question, or maybe to the panel. I cannot lose my constituent services. We do great constituent services in Tennessee 9. And this week on 11/14, Ryan Turner wrote me an e-mail, and he says, "I am writing as your constituent. As a constituent, I oppose this Stop Online Piracy. I am a student studying management of information systems. Should this pass, I believe my future IT would be crippled. Having a government hand in DNS service scares me, especially with the government suing website owners with 1(i)"—I think that was a misprint, but links, "as a content. As a college student who owns over 30 domain names, most of these places for third parties to post text responses, should one of those include a link to material that infringe copyrights, now I would be held responsible. I have no funding available. I handle these claims, and I am lucky enough to be trained on how to handle lawsuits, but many other entrepreneurs without formal training have no idea how to handle it."

If he had this and there was one text that came back that was maybe linked to an illegal site, would he be cut off, and what he then have to go to hire a lawyer and possibly go to court?

Ms. OYAMA. I think so. I think there are two ways that could happen. So, one of the concerns, you know, not just Google, but the other technology companies who endorse the testimony, the other trade associations, are concerned about is that the definition 103 of what is a site dedicated to fast is very broad. There is some language in there that also refers to a site or a portion of the site. So, people have a lot of serious questions about what does that really mean. Are we looking at a full site?

And today's Internet, the way most websites work, there is real time communication, and so you have read lots of real time comments. You have lots of real time posts. If one comment or post is infringing, does that, you know, impugn the entire site, or are we

looking at it holistically? There are some other words in the definition that give people concerned that it is overbroad.

So, either being swept in that way, or under the very broad immunities that are being given to service providers, pretty much anyone who qualifies under the definition of a qualifying plaintiff, which is very broad. They could go to a payment or advertising service provider. They could allege that the person that you mentioned is dedicated to theft, and then those providers have complete immunity to shut him off. So, there is a concern that there is a strong incentive in the bill that if you wanted to immunize yourself the easy thing to do would be to comply with that notice and shut them off.

Mr. SMITH. The gentleman's time has expired. And I do not mean to cut you off, but if you could bring your answer to a quick conclusion. Have you finished?

Ms. OYAMA. I think that is good.

Mr. SMITH. Okay.

Mr. KING. I think she could go longer.

Mr. SMITH. The gentleman from Arizona, Mr. Quayle, is recognized?

Mr. QUAYLE. Thank you, Mr. Chairman. And I want to thank all the witnesses for being here.

Ms. Oyama, I want to go back to what you were just talking about earlier about how long-term we can address the piracy issues via more legitimate websites that provide legitimate content on the Internet. And I want to go to your testimony that you indicated. The only long-term way to beat piracy online is to offer consumers more compelling legitimate alternatives. And you cited YouTube's free ad-based model for Monarch ties in content.

I mean, there could be some disagreement. I do not know what is the best way to monetize content, whether it is fee-based or free ad-based. And if you look over the course of history, except for broadcast, it seems like most quality content has not been given away for free.

So one thing that I want to ask you is, would you agree that the piracy issues that we are dealing with and the pirate websites that we are dealing with actually makes it more difficult for a company to start a fee-based site that offers legitimate content, and, thus, it forces content providers to look for ways that are going toward web and ad-based content to give it away for free?

Ms. OYAMA. I think there are so many different models in the ecosystem model right now. Certainly the problem of piracy is of tremendous importance and great concern to any content provider, right? You want to have control over the distribution of your content. Some people choose to release it for free because they want to participate with their friends and that way. Others want to license it, and others want to have an advertising model.

I think the kind of beauty, of all the new services that we are seeing is that there is no one-size-fits-all. I do think we would approach YouTube as a really great example of how kind of technology and copyright can work together. There is a tool on YouTube called Content ID. Because YouTube is a hosted platform, we host all the content, so it is on our servers.

So through Content ID, we are able immediately; a rightsholder would give us their file. If a user uploads a piece of content, we would immediately scanned 6 million reference files, and we could capture, if their song or their movie was being uploaded, and then the rightsholder would have control whether to monetize it.

Mr. QUAYLE. But I think might more direct question is that if we are not able to crack down and have the tools and the ability to crack down on the pirate websites, then you are actually forcing content providers into a narrow avenue of ad-based, providing only content via ad-based and free markets. Not free market, but free content.

Ms. OYAMA. So, both would be tremendously important, right, increasing license and piracy.

Mr. QUAYLE. Exactly. But, I mean, when you are looking at that and how we need to crack down on the piracy and ad-based, which is the model that Google uses, and that seems to be one of the reasons you would be pushing for that, because that is the way that Google makes their money, right?

Ms. OYAMA. There are different ways, but that is the primary way for sure.

Mr. QUAYLE. And I think that is just my biggest concern, is that if you are looking at just ad-based, you are cutting down one significant avenue for people to provide content. And if we do not shut down these pirate websites, then we are going to actually lose out on different types of business models, different types of content providers. And that was the point I wanted to make.

Ms. Pallante, I want to go to you. Earlier you stated in your opening testimony that you do not believe that the safe harbors under the DMCA are actually weakened by SOPA. Could you explant on that a little bit?

Ms. PALLANTE. Yes. First of all, the bill says that as a savings clause. And, secondly, there is no monetary relief. The injunctions that are allowed are already permitted under the DMCA. There are, contrary to popular belief, ways to enjoin certain action for certain action for search engines and ISPs. And really, this bill is really designed to sit next to the DMCA. The DMCA is related to particular files on a website, and does not require the participation of those who are really in a good position to help stem the tide of piracy.

So, I would object to a couple of things. I just heard from my fellow witness. One is that I am pretty sure that Google just said that it is the fault of content owners that we have a rogue websites. That just cannot be the truth. Secondly, although follow the money could be effective, it does not bring in everybody in the ecosystem. It does not bring in ISPs. It does not bring in search engines. It does not account for the vast number of websites that offer content purposely for free. And it does not really address the broader role of law issue that we have on the Internet right now.

Mr. QUAYLE. And under the DMCA, are there actually instances where a service provider can take down all content on a webpage or a website if there is infringing content on that website?

Ms. PALLANTE. The only way I see that happening is if every single rightsholder comes together at the same time, and approaches the website, and every file is infringing.

Mr. QUAYLE. So, it could be possible under the DMCA.

Ms. PALLANTE. It is highly unlikely.

Mr. QUAYLE. Okay. But the one thing I wanted to just get your final thoughts on, because opponents of the bill actually say that it is going to endanger the security and integrity of the Internet. One of the things that the Internet has been very good at is in commerce. And would it not also be fair to say that without shutting down these pirate websites, then we are also endangering the security and integrity of the Internet because they are putting out often counterfeit goods, and also infringed copyright materials?

Ms. PALLANTE. Right. So, there are three underlying purposes. One is to protect content owners about their own property. The second is to allow those who want to invest a place where there is sunshine and oxygen and a good environment for that. And the third is to protect consumers, absolutely.

Mr. QUAYLE. Thank you. I yield back.

Ms. OYAMA. Can I just clarify one point? I just wanted to make sure that nothing was mischaracterized, because I do not think that it is the fault of the rightsholders. Certainly, rightsholders have the right to protect their content however they want, and we are completely committed to going after piracy. My only point was that the success and the consumer appetite for services like Netflix and iTunes shows that there's are a lot of different licensing models out there.

Mr. O'LEARY. May I follow up on that, on one point, which I think is a practical point, which is being missed, to Mr. Quayle's question. There are legitimate services out there now, there are more of them than there have been before. There will be more of them tomorrow. The problem is that when you go to Google and you punch in the name of the movie, those legitimate sites are buried on page 8 of the search results. There is a better than average chance that Pirate Bay is going to end up ahead of Netflix. That is a fundamental problem, no matter how many legitimate sites are out there, that we cannot overcome, and we cannot do anything about.

If we could get Google to reach index of those sites in a way that favored legitimacy, to your question, Congressman Quayle, then consumers would be getting to those first. But when Netflix is buried way down in the search results, it does not matter how good Netflix is going to be, and that is just a practical problem that could be addressed today.

Mr. SMITH. Okay. Thank you, Mr. Quayle.

The gentlewoman from California, Ms. Chu, is recognized?

Ms. CHU. Thank you, Mr. Chair. I would like to ask about the savings clause, and I would like to ask both Ms. Oyama and Mr. O'Leary about your opinion on this. I am aware that concerns have been raised by Internet companies and many others that the language of the bill may have unintended consequences. And even though everybody agrees that the problem of foreign rogue sites is critical and that we need to cut revenue to these sites, there may be disagreement on the language as drafted. And I think it is really important that we try to reach some common ground, that we work through language that is balanced and effective, and make sure that we do not have unintended consequences.

One of the areas of disagreement on the Stop Online Piracy Act is on this question of the savings clause, and whether there is the immunity that is provided under the Digital Millennium Copyright Act for search engines and Internet service providers. And so, I would like to have your different opinions, because some have represented to me that the Senate bill has a savings clause. That seems to address this, but SOPA does not. And is that true? I would like to have your different opinions on this, Ms. Oyama and Mr. O'Leary.

Ms. OYAMA. Sure. So this is actually, it sounds technical, the savings clause, but it is of critical importance to the technology industry. Businesses today really build their business models under the safe harbors that they know they have under the DMCA. So, if a technology company receives notice of infringement, they are required to expeditiously remove that infringement, but they do not have kind of a general monitoring obligation.

So, the balance that we are trying to strike in any legislation would be if there are intermediaries who are required to do new things. Under this bill, that would be really clear—advertisers shut off your services, payments shut off your services. And that would be clear, and we would take those obligations. We want to make sure that this bill that is going after rogue sites does not strip us of those important safe harbors and kind of a related litigation and, you know, open the possibility that those types of orders could be used to establish red flag knowledge.

And so, there is some language that we propose that would kind of allienate that concern and keep this bill as effective as it needs to be to go after rogue sites. But a savings clause to make sure that we are not opening ourselves up to liability in a way that we would somehow be to proactively monitor all user generated content in real time is really important to us.

Ms. CHU. Mr. O'Leary?

Mr. O'LEARY. Congresswoman, I would just associate myself with the comments and the testimony provided by the Register of Copyrights. This legislation is a complement to the DMCA. It does not impute those rights or the safe harbor in any way, shape or form. DMCA deals with good actors, legitimate services that are trying to take steps to get infringing stuff off of their sites. Rogue sites deal with a group of people that under no definition would fit underneath the DMCA. They are bad actors. They are dedicated to infringement. These actually fit together. They complement each other. In no sense does this undermine the DMCA.

Ms. OYAMA. I think if that is the case, a one sentence clarifying that in any legislation would be tremendously helpful.

Ms. CHU. Ms. Pallante, what is your opinion on this, on the savings clause, and whether there are enough protections, and DMCA is not——

Ms. PALLANTE. Right. Thank you for the question. The question, again, is just—well, the problem is, just because somebody may be compliant under the DMCA does not mean that they should not take action if the Attorney General finds that there is a foreign infringing site run by criminals who are engaged in piracy. That is just an unfair comparison. And if that is the argument, this bill does allow for that, and it is my view that it should.

Ms. CHU. Okay. Well, I would like to ask a different question, and that is about job creation. There are some that are saying SOPA would stifle innovation and job growth, and that with an opinion, which was a finding by the U.S. Supreme Court that it contributed to infringement, that venture capital would try up.

But, Mr. Almeida, in your testimony, you noted that you represent over 4 million U.S. workers, and on their behalf that you actually support the Stop Online Piracy Act as an important jobs bill. How do you respond to these claims that this legislation would stifle innovation and job growth?

Mr. ALMEIDA. I think innovation is alive and well in the U.S., and I do not see this as stifling this in the least. Our members work in the United States. They are taxpayers. They go to work. They make products that we view as entertainment. That is what we see this online piracy infringing on. And you cannot hit a price point when someone is giving it away for free to make a business model to compete with free.

It also has to do with constructive innovation, and we believe in constructive innovation, like Netflix, as opposed to TV shack.bz, which is an infringing site that should be taken down.

Ms. CHU. Thank you. I yield back.

Mr. SMITH. Did you yield back?

Ms. CHU. Yes, I yield back.

Mr. SMITH. Thank you, Ms. Chu.

The gentleman from Texas, Mr. Poe, is recognized?

Mr. POE. Thank you, Mr. Chairman. Thank all of you for being here. This panel or this Committee is made up of former prosecutors, defense lawyers, and there are even two former judges here. And back in my experience on the bench down at the courthouse or the palace of perjury, as I referred to it in those days, I saw a lot of thieves. Stealing is stealing, and thieves are people we are to deal with. I disagree with you, Mr. O'Leary. They are not bad actors, they are thieves. And this legislation is trying to get a grip on this.

We have got really three groups that are here. We have the credit card companies, we have the search engine folks, and the content providers. If I had my way, I would lock all three of you in a room and do not come out until you all agree, then we could solve it, I would think.

If you pull up, as I did, if you pull up on the Google search engine "The Grinch Who Stole Christmas," or "Harry Potter," "free Harry Potter movies" or "free the Grinch Who Stole Christmas," you get a lot of free sites on there. And as a consumer, I cannot tell who is a thief and who is not a thief. And I know Google is doing a lot, millions of sites and all of that. I have heard the testimony. But at the point we are now, what can Google offer to this bill that Google would sign on to the bill, specifically?

Ms. OYAMA. Sure. So, to your point about the search results, one of the major commitments that we made this year was to improve the tools to make sure that when rightsholders notify us those search results will be disabled in the search. And so, the commitment that we had made at the beginning of the year was to reduce the turnaround times to under 24 hours. And so, we are happy to say right now it is 6 hours or less is the average turnaround.

In terms of what we could do affirmatively——

Mr. POE. Yes, from this day forward. You pull up "The Grinch Who Stole Christmas," and you keep going page after page for free Grinches.

Ms. OYAMA. So long as those sites are there, they are going to show up on the Internet. And so, we think that legislation that would target the source of those sides is necessary. What we would do is we would support legislation that would go through the Department of Justice, so you would have law enforcement on that. You would have a court determined that a site is dedicated to infringement, and you could serve those orders on U.S.-based payment providers and advertising.

We have Google Checkout for payment. We have AdSense, AdWords, a lot of different advertising products that would directly regulate and impact our business. But we think that if we can break the financial ties for those sites, then, that really is smart, targeted, and effective, and would avoid some of the collateral damage that we have discussed earlier this morning.

Mr. POE. So, your answer is just go after the finances.

Ms. OYAMA. Cut off the funding.

Mr. POE. Yeah, cut off the money. So, if that were something that we added to the bill that would cut off the money, then Google may support it. Is that what you are telling me?

Ms. OYAMA. Yes. There are certainly concepts in the bill that reflect that. But we think if you look at Wikileaks, that is how they have been taken out is by cutting off the money. It is an approach that U.S. law enforcement uses for many in different international problems, you know, narcotics, terrorism. I mean, it has been a proven way. If you cut off someone's financial incentive, they are not going to want to pay for the servers, and the bandwidth, and the infrastructure to run these websites.

Mr. POE. Okay. Let me be a little more specific. What can Google do, not what the financial providers can do, what can Google do to move this legislation forward?

Ms. OYAMA. So, there is a lot we are doing in the private sector, but in terms of the legislation, we would publicly support legislation like what I described, follow the money approach. We would be happy to do that. We would be happy to work with your staffs on legislation in that way, if it can avoid the collateral damage that we have discussed, and if we got a good definition of what is a rogue site, that did not sweep in legitimate U.S. businesses.

Mr. POE. But you cannot tell when you pull it up, "The Grinch Who Stole Christmas," who is the real grinch is and who is not. You get page after page of free Grinches.

Ms. OYAMA. That is why is court adjudication or a collaboration with rightsholders is really important. There are lots of legitimate free movies. There are lots of heat, you know, content that just the middleman would not really know if that was licensed or infringing.

Mr. POE. You want in on that, Mr. O'Leary, and then Ms. Pallante.

Mr. O'LEARY. I think, to use the example of the Grinch, there is a movie right now, as I mentioned earlier, called J. Edgar. The only lawful place you can see that movie is in a theater. If you go back

to your office and put "J. Edgar" into Google, you are going to get the same list of eight pages of sites where it is free. That movie is not available for free anywhere. If you want to see it, you have to go to a theater right now.

So, I understand the complexity when you are talking about something that is perhaps not in the theater, but this is actually in the theater right now, and there is no reason for it to be online in any fashion frankly. I also think that what is being proposed, what was being suggested is, as I said earlier, we should follow everybody's money.

And isolating one or two things, that does not solve the search engine problem that we have been talking about, and we think that should be a part of the discussion to. We think it requires all of the people who are involved in this to work together to get it done, kind of to your theory of throw everybody in a room and sort it out. If everybody does not go into the room at the beginning, you are not going to get it sorted out.

Mr. POE. Maybe we need a court order to get you all three in a room.

Thank you, Mr. Chairman. I will yield back.

Mr. LUNGREN [presiding]. Thank you. Maybe get the FBI to help you on that J. Edgar Hoover stuff.

Mr. Deutch, you are recognized for the next 5 minutes?

Mr. DEUTCH. Thank you, Mr. Chair. First of all, it is not just J. Edgar. I have teenaged daughters who are awfully excited about the new Breaking Dawn movie, which is coming out. You can watch that right now online for free.

What troubles me about this a whole exchange, quite frankly, is on the one hand, there is this great technology, Ms. Oyama, that you have so proudly trumpeted, understandably, about YouTube and what YouTube does in order to prevent illegal content from being posted. Yet when you enter "watch Breaking Dawn for free," and you can do it online now, there you throw your arms up in the air. Well, there is nothing we can do.

Ms. OYAMA. Sorry, I can understand how that would feel frustrating. Technologically there is a distinction. So, on YouTube, the content that is posted on YouTube is hosted on our servers, so we are able to match files. If someone tries to upload something on YouTube, we have a reference file we can match against. We do not control the World Wide Web.

Mr. DEUTCH. I understand that is a technology issue. We could talk more about that. I have another question for you. This has been a fruitful exchange, different than I might have expected from the way, as a number of us have read referenced already. The way this debate has played out in the local press in particular, I do not know whether Google shares the position publicly that this bill will kill the Internet and all of the advertisements that have resulted, and all the phone calls that we have received in our office. But I do wonder if there is any base level here that you would agree needs to be tackled.

And so, if the issue is the language that says a "portion thereof," let us assume the bill did not have that language in there. So you cannot argue that Twitter would have to be taken down, which, by the way, is an argument, there is no basis for that argument.

Under this bill. You cannot argue under this bill, that Facebook would have to be taken down. There is no basis for that under this proposed bill. And I think that you understand that, notwithstanding the reference to individual tweets that might lead a whole site to be taken down.

My question is, if that language were not in there, are there any of these websites that you believe should be taken down and that Google ought to play a role in helping us accomplish that?

Ms. OYAMA. Yes. We would be happy to work with the Chairman, with your office, on a follow the money legislation.

Mr. DEUTCH. Okay. Well, I understand. So, you do not like the way the bill is written. Let me ask about that because you have many references to day to following the money. Yesterday, your Chairman recommended regulations based on tracing payments at websites offering illegal materials as a replacement for this bill, consistent with what you said today. Many of the offshore sites clearly engaging in that are driven by, as you point out, are driven by ad revenue, not just credit card transactions. And if we follow the money, we cannot just focus on the credit cards obviously. We have to focus on the ads.

Google, at least from the statistics I have been told, retains over 75 percent of all search advertising revenue in the U.S., therefore, following the money leads us to you. So, tell me the steps that Google has taken already, understanding that you are concerned about this intellectual property theft, understanding the impact that it is going to have every day on our economy, tell me the steps that Google has taken to combat it using the following the money approach that you favor.

Ms. OYAMA. Okay. So, just to confirm, legislation that would go after ads is a big part of our business.

Mr. DEUTCH. I understand, but given——

Ms. OYAMA. And we are happy to support that.

Mr. DEUTCH. I understand that, but tell me what you have done——

Ms. OYAMA. Okay.

Mr. DEUTCH [continuing]. Now, because we all acknowledge this is an important issue. And if a 75——

Ms. OYAMA. And one should not prevent the other, right.

Mr. DEUTCH. Right. You can play a significant role today. So, if you could just speak to what I have already done.

Ms. OYAMA. Okay. So, there was some major commitments that our General Counsel, Kent Walker, made at the beginning of the year. I will just try to tick off the major ones, but we should probably follow up with your office on more specifics.

For DMCA, we have removed more than 5 million infringing files. This year, when rightsholders notified us. One of the concerns we have heard is that there were some grit in the system, and that there was frustration that it was taking too long. So, we invested significant engineering hours and money to improve the tool.

Mr. DEUTCH. Ms. Oyama, I hate to cut you off. I do not have a lot of time here, but I would ask that you would follow up. I remember Mr. Walker's testimony. I followed up with a letter after that hearing requesting all sorts of information. I have not received

a response. So, I hope that a response will be forthcoming to that letter and to the request that I have made here today.

I would like to finish with this. This notion that we are going to break the Internet, that somehow we are going to stifle innovation, the fact that the kid serving me coffee at Starbucks told me, "hey, I hear you are taking up legislation that is going to make it impossible for me to download music." The fact is what we are worried about is, and the reason we are having this discussion, what we are worried about is not stifling that innovation in the future. That is a concern that we all have. And I do not believe that the legislation does that. But we know right now if we do nothing, that the film industry and those young directors who are starting out, are not going to be able to do their craft, and we are not going to have the next Dell, or we are not going to have the next Drake, because they are not going to be compensated for their work.

And I hope that as we go forward in this that you provide those answers, that we can have an honest discussion about what is really at stake here, and let us move past this. These attacks on those of us who believe this, and suggest that somehow we are going to mean an end to the Internet, it is not accurate. I think you understand that it is not accurate, and it does not do the American economy any great service at all.

And with that, I yield back.

Mr. LUNGREN. The gentleman yields back, and the other gentleman from Texas, Mr. Gohmert, is recognized for 5 minutes?

Mr. GOHMERT. Mr. Chairman, again, also appreciate your being here. It is a tough subject, and we are dealing with intellectual property here. And, I, like my friend, Judge Poe, was a District Judge and also a Chief Justice. And we dealt with, it was not called bad actors, you know. You dealt with that, and that is really what we are talking about here. It is a crime. It is theft. We do not want thieves working their way through an honest, legitimate, wonderful means of, in this case, the Internet.

In the past, some have used the example of the pawn shop cannot intentionally and knowingly assist in that effort. And so, there were laws made. Most States have them where law enforcement can go in and get information. And I know, and I have been resistant to some of the pushes to force Internet providers, search engines, into doing things that we do not even require pawn shops to do. And I thought some were going overboard in trying to make demands on search engines that we do not even demand of pawn shops.

But, on the other hand, there is this aspect of our criminal law, and every State has it, the Federal Government has it. Anyone who aids, abets, encourages, in any way assists someone in committing a crime, the law is very clear in every State and the Federal Code, you are just as guilty as if you committed the crime yourself.

The question is, do you intentionally or knowingly aid. Well, it has been brought up often enough. There are thieves using the Internet. And I keep hearing from people who say, look, if it were illegal for me to use that free website, then how come I get access so easily? They are expecting us to do something. And I think most of us were hoping that there would be something worked out between the interests here.

But I can give you an example. I know what the law is, and I had an eight track "Warm Shade of Ivory, Henry Mancinci" back in college, and it got me through some all-nighters, that and "Jonathan Livingston Seagull" soundtrack. So, anyway, Sleepless in Seattle has this song in the wee, small hours of the morning. And I wanted to get that. I wanted to download it. I would pay for two bucks for it, not just 99 cents. Nobody has it except some free websites I knew not to go use those and download it free because it is illegal. Most people do not.

So, when we talk about follow the money, we are talking about something terribly difficult in going to China, going to Russia and trying to follow the money over there. We are not getting help from those folks. Marsha Blackburn and I met with their folks in China that handle this stuff, and it seemed pretty clear to me we were not going to get a whole lot of help out of them.

So, what should we do to keep from hurting the innovation of the Internet, and Google, and Bing, and these folks that come up with great ideas, but at the same time balance the interests in this being a law abiding society. And I am gratified to hear people on both sides of the aisle have similar concerns.

So, it just does not seem to me to be that onerous to say if someone goes to court, for heaven's sakes, and proves with probable cause standard that somebody is committing a crime of theft, and then that is presented to an Internet provider or search engine, these people are committing a crime. There is probable cause to believe that is justification for a warrant, why that is too onerous to say do not make them accessible. And I am still having trouble understanding that, and I would welcome comments in that regard from whoever wishes to. Thank you.

Ms. OYAMA. Thanks. I think we completely agree about the importance of having a Federal judge play the role of an arbiter so that folks' services are not being terminated just by a 5-day notice to their provider without the ability to appear and defend themselves.

I think to your point about what we can do, it is probably three things. So, one would be building on the DMCA. Under the DMCA today, search results can be line edited out if a rightsholder tells us, a search engine, to remove a piece of content. We have worked incredibly hard over the last year to improve our tools. The average turnaround time today is 6 hours if we receive notice.

So, we are working really hard on improving that. It is not perfect. It is not done. It is something we will continue to work on.

The second piece, though, would be to build on that and to come together and support legislation that would impose new obligations on other providers. So, we are also an advertising provider, largely an advertising provider, a payment provider.

A judicial process where a court determined that a site was dedicated to infringement, and then instructed U.S. based intermediaries to shut off financial ties to that website, that is the most important and effective thing we could. If we can knock them off at their knees and we can cut off their financial ties, they will not have a reason to be in business anymore. They will not be making money. That is the effective way to go.

And then the third piece would be to get rid of ineffective and harmful pieces. So, I realize reasonable people can disagree about this, but there a tremendous concern in the technology industry about some of the remedies that are being proposed and some of the unintended consequences that would have, you know, potentially very severe repercussions for the Internet network, for people's security, and for free speech concerns.

So, getting the balance right is something we think is important. We certainly think that there is a way forward and a way that we could agree on going after these sites.

Ms. LOFGREN. Would the gentleman yield?

Mr. GOHMERT. Well, I would ask unanimous consent to allow others to finish answering because there are a couple of hands. And I certainly——

Mr. LUNGREN. The gentleman is extended another minute.

Mr. GOHMERT. You had requested to comment.

Mr. CLARK. I would just add that in regard to your comments about thievery and Congressman Poe's, from our industry's perspective, it is more than thievery. It is murder. We do feel, I particularly feel, and I have 28 years of Federal law enforcement, I know crime when I see it, and I see counterfeit medicines as actually attempted murder. I mean, it is not quick, it is not immediate. But when you are only giving a patient 20 percent of the medicine they need to cure their cancer or their heart problems or their high blood pressure, you are, in fact, killing them slowly. But that is the issue here.

Mr. GOHMERT. As a prosecutor, you know that may be not be murder, it may be negligent homicide or some other type of homicide.

Mr. CLARK. Along those lines. And it is frustrating. If we are not immediately making progress in cutting that down. I have worked with CDP and pilot programs, and I am seeing counterfeits flooding in because of the purchases over the Internet from the rogue websites that are selling counterfeit medicines. And it is incredulous to me how much is coming into the United States.

So, I would say, you know, this bill is going forward with demonstrating that we need to change the status quo. We cannot accept what is existing right now. And I agree very much that we have to demonstrate to people that there are consequences, and this is a serious crime. When you look at 6 months, 4 months, 3 years. You say your cost of doing business, it cannot be that bad if that is all they are going to give.

So, I also see the Title II in this as very, very significant as well.

Mr. GOHMERT. Was there anybody else that wanted to comment? All right. Thank you.

Ms. LOFGREN. Would the gentleman yield?

Mr. GOHMERT. Yes.

Ms. LOFGREN. I just wanted to briefly, I think it was Mr. O'Leary suggested that if you type in "J. Edgar movie" you get all these infringing sites. And I just did that, and what you get is the show times in Washington, a review, the Wikipedia article, the trailer from Warner Brothers, several reviews of the movie, the iTunes trailer. There is not a single infringing site that comes up. So, I just thought we——

Mr. GOHMERT. Reclaiming my time——

Mr. MARINO. Would the gentlewoman or the gentleman yield?

Mr. GOHMERT.—I think if you use the word "free" in there, that is where those things come up. But, yes, I will yield.

Mr. MARINO. Would you yield? Well, I just did the same thing, and on——

Ms. LOFGREN. Did you use Google?

Mr. MARINO. I just Googled it, "watch J. Edgar Hoover free online," on YouTube, full versions. It shows you how to download it, no cost. Right here. There is a list of——

Ms. LOFGREN. Well, I did a different search engine. But the point I am trying to make going back——

Mr. GOHMERT. Well, reclaiming my time, I do not know what——

Mr. LUNGREN. The gentleman's time has expired.

Ms. LOFGREN. I would ask that the gentleman be granted 15 seconds and so I might say just in answer to—the point is the search engines are not capable of actually censoring the entire World Wide Web. That is the problem. You cannot do that. And so, we need to go after the people who are committing crimes in a way that is going to work. I think we can do that, but this bill is not it. And I thank the gentleman.

Mr. GOHMERT. Reclaiming my time——

Mr. LUNGREN. The gentleman's time has expired.

Mr. GOHMERT. I agree, but also need to cut off the getaway. And with that, and I am not sure what the gentlelady has against Google, but I respect her using Bing, and yield back my time.

Mr. LUNGREN. The gentleman yields back time he does not have. [Laughter.]

I am going to accuse you of being a liberal here in a minute.

Mr. Johnson is recognized for 5 minutes?

Mr. JOHNSON. Thank you, Mr. Chairman. Mr. O'Leary, SOPA requires payment networks, like MasterCard, to suspend payment transactions between a U.S. customer and an online merchant within 5 days. According to Ms. Kirkpatrick's testimony, there are very legitimate challenges that payment networks have in meeting such a short deadline, especially considering the multiple players involved in an online transaction.

The Senate version requires payment networks to take action as expeditiously as reasonable. Earlier this year, the White House negotiated a best practices document with the payment industry that has a reasonable period of time standard.

Which of these standards is acceptable to you that within 5 days under SOPA the "expeditiously as reasonable" under the Senate version, and a reasonable period of time as negotiated between the White House and the payment industry?

Mr. O'LEARY. Yes, sir. I think it is a legitimate question, and one that we believe can be resolved favorably to everyone.

Mr. JOHNSON. Which one do you think is most acceptable to you?

Mr. O'LEARY. As I sit here right now, I am not prepared to pick between the three, quite honestly. I certainly understand the point that was made by our colleagues at MasterCard if it is not possibly done within 5 days. We certainly do not want to create a time limit which forces them into an impossible standard.

Mr. JOHNSON. All right.

Mr. O'LEARY. At the same time, we would like the legislation to recognize that if someone is trying to run the clock out, they do not do it.

Mr. JOHNSON. If I open up the tent for you to stick your nose in, boy, you are going to get all the way up in there. I am just appreciating your gift of gab.

If I might ask Mr. Clark the same question.

Mr. CLARK. I feel the same way.

Mr. JOHNSON. Okay. All right.

Mr. CLARK. Sorry. I feel the same way.

Mr. JOHNSON. All right. Ms. Pallante, Section 506 of the Copyright Act establishes criminal liability for the willful infringement of a copyright. Recently, there has been confusion as to the definition of that term, "willful." Do you think that willfulness is the same as intentional? Tell me about the difference between those two standards.

Ms. PALLANTE. Right. So, that is a great question, and the point of SOPA is to capture those that knowingly engage in a known legal duty. And that is the standard that most courts have accepted. There are some exceptions to that. I think that is something that could be clarified in the bill, in legislative history perhaps.

Mr. JOHNSON. All right. Ms. Oyama, the DMCA in Section 230 of the Communications Decency Act represent the legal underpinnings of the view that intermediaries need not monitor or supervise the communications of users. It is a view that we have long touted and pushed across the world through various diplomatic channels. We have harshly criticized governments who use such virtual walls to prevent citizen access to the Internet. China is a great example. With that in mind, would this legislation allow companies to demand that search engines located inside the U.S. censor where American consumers are able to go on the Internet? And how would this legislation likely be viewed by China, and Iran, and other countries that put these roadblocks in terms of content to their citizens on the Internet? And how would that affect our diplomacy?

Ms. OYAMA. Thanks. So, for the DMCA piece that you mentioned, I think we would certainly agree that DMCA has proved to be a foundation for American innovation, and has struck a balance. So, if you are a new company or starting up, you know what the laws are. You have certainty. And it also helps rightsholders. If a rightsholder is aware that there is infringing content on the service provider, they just need to let us know. Web hosting companies search and engines. We will remove access to that content. It strikes the right balance. It takes care of infringing speech. It leaves up legitimate speech. And it reflects a careful balance. And also, because of the way web services are used today, we see all over the place when there are real time events, it is important that a web platform enables that type of real time communication, of real time e-commerce.

If you did not have the DMCA and an intermediary platform was required or potentially liable for what its users were posting in real time, you would have to implement some type of proactive monitoring system. It could really change the dynamics of the Web today.

I think the second piece——

Mr. JOHNSON. That would stifle the small entrepreneur that is just getting started, more than it would hamper the larger providers of content.

Ms. OYAMA. I think it is both, but it certainly——

Mr. JOHNSON. It would be a burden on both.

Ms. OYAMA. Yeah. If you are a new company starting up, you will have less money to invest in that type of monitoring. So, certainly, it would have an impact on small businesses.

To your question about, you know, kind of the speech aspect, you know, if we impose a law here, which would have court orders requiring of domestic search engines to make entire full websites disappear, and especially if there is some type of overbroad definition which would capture also legitimate speech, you know, unfortunately, what we do here would have other ramifications. And we may think that this is a good reason, we do think this is a good reason here. But we see all the time for Google DMCA requests. Competitors tried to take each other down. Pro-democracy speech tries to be quelled. We have seen in Libya and the recent activities there, different politicians tried to take each other's YouTube channels out because they disagree with their views. We see copyright use all the time as an excuse to quell speech.

If we mandate this type of approach here, we really need to think carefully about what types of international ramifications that will have on free expression globally.

Mr. LUNGREN. The gentleman's time has expired.

Mr. JOHNSON. If I might get just one more question.

Mr. LUNGREN. All right. The gentleman has already had extra time, but so has everybody else, so go ahead.

Mr. JOHNSON. Thank you. Thus, Justice Department has responsibilities under the SOPA act. While at the same time, we have been talking about downsizing government, and, in fact, the Justice Department has lost about 30 percent of their attorneys. How does this affect the effort to criminally go after these pirates, and also from a civil standpoint? I will ask that to Mr. O'Leary.

Mr. O'LEARY. Well, I think that, you know, this bill actually speaks directly to that point. That is part of the reason there is the ability for individual plaintiffs to move so that the burden does not fall solely on the Justice Department.

The content industry, Pfizer——

Mr. JOHNSON. What about the criminal part, though, because we get people being prosecuted for shoplifting and stealing little small petty items. But this is multi-billion white collar fraud, which only the Justice Department has or should have the, really had the resources and the breadth of law enforcement ability to address. How does the downsizing of the Justice Department impact criminal prosecution?

Mr. O'LEARY. Well, I think as a general premise, would you downsize the Justice Department, obviously it has an impact. But let us be very clear. The Justice Department does pursue criminal cases internationally.

Mr. JOHNSON. Well, how can it do so——

Mr. LUNGREN. The gentleman's time has expired.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. LUNGREN. Some time ago. Recognize myself for 5 minutes.

Mr. JOHNSON. Well, I am a liberal. [Laughter.]

Mr. LUNGREN. Well, I would not accuse you of being anything else. [Laughter.]

Mr. JOHNSON. Well, I bear that shame with great honor. [Laughter.]

Mr. LUNGREN. This is sort of a reverse to the old story that I went to a fight and a hockey game broke out. I came here as one who has not made up his mind on this bill, hoping to receive information on this. And I think everybody on this panel is committed to fighting piracy. I mean, maybe I am the only Member of this Committee who has got a gold record. I got it from the recording industry for my work on anti-counterfeiting. When I was attorney general of California. So I very much believe there is an important role for us to play, law enforcement, in civil law in this regard.

But my concern is something that was brought to my attention as the Chairman of the Cybersecurity Subcommittee on Homeland Security, and that is the existence of a system that has been going on for some years, called DNS security or DNS-SEC. And I have heard from some of the engineers who have been working on this in the Internet area that we of applied this law in this way, it would undo what we have been doing it to try and secure the Internet by way of DNS-SEC or DNS security. So, I would like to ask the panelists if any of you feel you can speak to this point, because it is one that was raised with me. I am not a technical expert on this, but there was some real alarm by Internet engineers, I would call them, who really do not have a dog in this fight and in terms of the disputes between the various special interests here. And I mean that in the proper way, special interests.

And so, what I ask Mr. Clark, for instance, are you aware of this criticism, and does this legislation, would it incentivize Internet service providers from using the DNS security extensions because it mandates the redirection of customers to another website?

Mr. CLARK. No, I am afraid I do not. I am not familiar with that.

Mr. LUNGREN. Okay. Mr. O'Leary?

Mr. O'LEARY. Well, I am certainly aware of the argument, and the people that we have talked to, it is a concern, which is, frankly, overstated. As I mentioned earlier in response to another question, there are numerous countries around the world that engage in this type of activity. The Internet has worked without a problem in regard to that. And I think also, you know, they are overlooking and looking at this debate. There is an existing security problem with the current state of play, and that is these rogue sites taking private information from consumers and spreading malware and spyware and things like that.

The final thing I would say is that in regard to other things, like dealing with malware, dealing with spyware, dealing with child pornography, this type of activity occurs all the time, and the Internet seems to function just fine.

I tend to agree with the comments of Mr. Deutch that if the Internet is going to be all things to all people, it should also be in terms of trying to help us stop people from stealing our stuff. The problem, frankly, is that the Internet seems to be for trade——

Mr. LUNGREN. Well, that is not my point. My point is whether or not you can respond to the specific question raised by Stewart Baker, former DHS Assistant Secretary of Policy and former NSA General Counsel, to the effect that if this approach to respond to a legitimate problem were put into effect, it would undercut an effort that has been going on for nearly a decade to secure the Internet by way of this program that I referred to.

Mr. O'LEARY. We disagree with that position.

Mr. LUNGREN. Okay. Can you submit in writing for us specifically how you disagree with that approach?

Mr. O'LEARY. Certainly, I would be happy to.

Mr. LUNGREN. Ms. Kirkpatrick?

Ms. KIRKPATRICK. I am unfamiliar with that element. I am unaware of it. I do not have the technical expertise to comment on it.

Mr. LUNGREN. Does anybody with your organization have the expertise?

Ms. KIRKPATRICK. I certainly can follow up and get back to you.

Mr. LUNGREN. Would you please respond to that specific question, because to me it is an underlying question that is extremely important, having worked on the problem of cybersecurity. If what we are doing here has the unintended consequence of upsetting what is, at least in the opinion of a number of experts, and they may be wrong. I am trying to ferret this out, undercut a real effort that would practically help us secure the Internet, that is bothersome to me.

Ms. Oyama?

Ms. OYAMA. Sure. So, I think the concerns that you mentioned are the ones that we have heard as well, from many cyber security experts. I knows Stewart Baker has written about this. The designers of DNS-SEC themselves have published a white paper. I am not—yeah.

Mr. LUNGREN. Do you have anybody that has expertise with your association and can respond to that specifically, because this is not part of this hearing, and I am very concerned that evidently this bill is not being referred to my Subcommittee. And I am not parochial about this, but if we are going to do it, we ought to at least talk about it and to have people come in here and say, well, our organization—either we do not take a position or we are not experts on this is upsetting.

Ms. OYAMA. I think that there is great concern within our company.

Mr. LUNGREN. Well, could you please respond in writing on that?

Ms. OYAMA. Sure, happy to.

Mr. LUNGREN. Could you, please?

Ms. OYAMA. Yes.

Mr. LUNGREN. And, Mr. Almeida?

Mr. ALMEIDA. No, no expertise.

Mr. LUNGREN. Okay. Ms. Pallante, do you have any?

Ms. PALLANTE. I think that Congress should absolutely consult objective technical experts. But I will add is that ICE, through operation on our sites, has been using the existing seizure and civil forfeiture laws to essentially disappear website in the United

States. So, this bill would take that criminal standard and apply it to foreign sites.

Mr. LUNGREN. Thank you very much. Let us see, who is next? Mr. Marino is next for 5 minutes?

Mr. MARINO. Thank you, Chairman. Thank you, ladies and gentlemen, for being here. I think my colleague and friend, Ms. Lofgren, and I pointed out a very good example of how easy it is. This is on some sides and not others. I think so. Zoe went to Bing and got the trailers, and I went to Google, typing in "free," who sent me to YouTube for the free movie. So, you know, there is a lot of work to be done here.

Ms. Oyama, I want to compliment you on your decorum and your professionalism and your loyalty to your company, for being here and answering the tough questions that you have been answering. You are certainly an asset to your corporation.

Ms. OYAMA. Thank you.

Mr. MARINO. Nevertheless, I think it is reprehensible that the chairman, that the CEO, that the president, that the counsel, none of them thought it was responsible enough for them to be here, and they sent you into the lion's den. And you certainly deserve a large portion of their bonus at the end of the year.

Ms. OYAMA. Can I just add one thing to your question on our general counsel, he was here in the spring. He cares very much about this problem and doing it the right way.

Mr. LUNGREN. Good.

Ms. OYAMA. He, I think, sent a letter saying he had a long standing personal commitment for today, any other day, he would be here, and he looks forward to continuing——

Mr. MARINO. All right, I give that to him, and I remove his name from that list, and he can keep his bonus, all right?

Let me ask you a question here. I want to thank Google for what it did for child pornography, getting it off the website. I was a prosecutor for 18 years, and I find it commendable. And I put those people away. So if you can do that with child pornography, why can you not do it with these rogue websites? And let me follow that up with, why not hire some whiz kids out of college to come in and monitor this and work for the company to take these off?

My daughter, who is 16, and my son, who is 12, we would love to get on the Internet, and we download music, and we pay for it. And I get to a site, and I say, this is a new one, this is good, we can get some music here. My daughter says, "Dad, do not go near that one, it is illegal, it is free, and given the fact that you are on the Judiciary, I do not think you should be doing that." So, maybe we need to hire her. But why not?

Ms. OYAMA. So, the two problems are similar in that they are both very serious problems. They are both things that we all should be working to fight against. But they are very different in how you go about combating it. So, for child porn, we are able to design a machine that can detect child porn. You can detect certain colors that would show up in pornography. You can detect flesh tones. You can have a manual reviewer. Someone would look at the content and they would say this is child porn, and it should not appear.

We cannot do that for copyright just on our own because any video, any clip of contact, it is going to appear to the user, to be the same thing. And so, you need to know from the rightsholder, the owner of the right, how have you licensed it, have you authorized it, or is this infringement.

Mr. MARINO. I only have a limited amount of time here, and I appreciate your answer. But we have the technology. Google has the technology. We have the brainpower in this country. We certainly can figure it out.

Let me move on here. First of all, Mr. Clark and Mr. O'Leary, I want to thank you for your dedication to law enforcement. I have been down there for 18 years, and thank you so much. And, Mr. Almeida, my father was a fireman for 30 years, so I know exactly what you are talking about. So, I want to pose this question to anyone.

It is my understanding that taking down a portion of the site is much more difficult than taking down the entire site, so I am hearing from the testimony here. So, is there a more balanced approach that we can assist you in letting you take the lead on it in defusing of this problem and stopping this infringement on these materials, this illegal stealing of our materials that is costing us jobs and is costing this country a lot of money? If you understand my question, please jump in, anyone. I do not think anyone understands my question. [Laughter.]

Ms. Pallante?

Ms. PALLANTE. Well, no, I appreciate the question. I do not know the answer. Certainly, when law enforcement goes before a judge and tries to get a court order that would allow it to seek relief from the website, and then engage the search engines, the ISPs, the payment processors et cetera, to help, they would like to stop the infringing material and not be non-infringing material. I do not know if it is a technical solution, or if it is just a question of each website, having different pages where they can easily find the infringing content.

Mr. MARINO. Do any of you agree with me that we do have the brainpower and the technology available to figure this out, if we want to spend the money?

All right, thank you, and I yield back my time.

Mr. LUNGREN. Great. The gentleman's time is up.

Mr. Amodei, you are recognized for the last 5 minutes of this hearing.

Mr. AMODEI. Thank you for that strategic timing of my recognition, Mr. Chairman. I appreciate that. And so, in honor of your discretion, I will not use the whole time.

I would like to, first of all, associate myself with the comments of my colleague from California at the of the dais, Mr. Deutch. I think he has hit the nail on the head. When you are the last guy, you do not want to try to see if you can prolong things any more than usual.

I would like to ask the Chair, however, since there is written responses to this security thing, and I tried to write the guy's name down. I am new; I do not know. Maybe it was Stewart Baker? Maybe we could have Stewart Baker's concerns written so we can

have something to compare those with. And if that is out of order, then I will shut up on that and move right along.

Mr. LUNGREN. Mr. Baker's article was made part of the record. [Laughter.

And the gentlelady from California is giving it to you right now.

Mr. AMODEI. Okay, good. Thank you.

Mr. LUNGREN. And if I were Chair, I would have him here, but I am only temporary Chair. [Laughter.]

Mr. AMODEI. Thank you for your compassion for someone who has been here for 61 days.

Finally, so that I have something to yield back, I appreciate the concerns. This strikes as one of those deals where the pursuit of the perfect is going to get in the way of the good. One thing, and I apologize for missing the part that I missed, but there was an opportunity to talk with some folks in another Committee that was kind of important. But I did not hear anything that said, "no, this is not an issue; no, this is not taking place; no, those jobs, or this gentleman on the end, are not being threatened; no, it is not real time impacts when Mr. Marino can dial in and be watching it right now."

Quite frankly, I think there is an issue—I do not how you address it because nobody should leave the room thinking I am technically savvy. But I do not have anything to type on, as a matter of fact. They even took my iPhone away today.

But I will tell you this. The impacts are instantaneous. Once it is downloaded, it is gone. That horse is out of the barn, and it is never coming back. And when you have a broken leg, you need to go to the hospital.

And I agree with Mr. Marino's comments. Way to go. Whatever they are paying you, it is not enough. And so, if those pansies want to come by someday and say hi, tell them they are welcome. [Laughter.]

So, anyhow, when your leg is broken, you got to go to the hospital, and unfortunately you are in the medical business on this stuff, and so I can just say that my concern is this. You are a major operational piece of this. The criminal activities are uncontroverted that are happening, and to do nothing is wrong. Nothing happens quick in this process. I believe from my vast amount of experience, and so it is time to try something.

And so, while I appreciate the concerns, when I hear the recurring think of follow the money, there is plenty of money around to follow. And that is a good thing. I am a Republican; it is a good thing to make money.

So, I will just tell you from my perspective, it is time to move. If there was a perfect bill that ever came out of here, it will sure be neat for me to be here while it happens, but I am guessing it is not going to happen when I do. So, I would appreciate best recommendations so that we can get moving on in terms of stopping something that is taken 7 years just to get to this point. I am not picking on you.

And so, with that, Mr. Chairman, I see the light is where it is. I yield back the most time that anybody has yielded back today.

Mr. LUNGREN. Very good. The gentleman will be commended.

I would like to thank our witnesses for the testimonies today. Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record.

We thank you all. We appreciate your testimony on a very difficult subject.

This hearing is adjourned.

[Whereupon, at 1:29 p.m., the Committee adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Ron Wyden, a U.S. Senator from the State of Oregon

I would like to take this opportunity to commend Chairman Smith and Ranking Member Conyers for holding this hearing. While I would have liked to see a more diverse range of voices included at today's table, I appreciate the opportunity to share my views on this important subject.

While some would like to paint this issue as a simple matter of being for or against intellectual property, that would be a mistake.

Believing that a free and open Internet is worth fighting to protect does not mean that we aren't concerned about copyright infringement or that we are somehow oblivious to the fact that unscrupulous foreign suppliers are using the net to traffic counterfeit and illegal goods. They are and Congress and this committee are right to be considering remedies to stop them and to protect the hard work of our creative industries.

Rather, those of us who value the Internet's growing role in our society recognize that any government intervention in the online ecosystem that is the Internet can and will have a ripple effect on more than just its bad actors. Interfering in the Domain Name System (DNS) for example would undermine the net's structure and harm cybersecurity efforts. Authorizing a private right of action, for example, wouldn't just allow rights holders to use the courts to protect their intellectual property. Companies could also abuse such authority to protect out-dated business models by quashing new innovations in their infancy and discouraging less than complimentary speech.

In other words, the wrong approach to combating infringement could fundamentally change the Internet as we know it, moving us towards a world where transactions are less secure, ideas are less accessible and starting a website wouldn't be an option for anyone who couldn't afford a lawyer.

The Internet has become an integral part of our everyday lives precisely because it has been an open-to-all land of opportunity where entrepreneurs, thinkers and innovators are free to try and fail. The Internet has changed the way we communicate with each other, learn about the world and conduct business, because instead of picking winners and losers, we created a world where every idea has an opportunity to be heard regardless of where it originates.

As Members of Congress we can now engage with our constituents via online innovations in social media, while a small business in rural Oregon can use the Internet to find customers around the world. And the Internet isn't just becoming the global marketplace for goods and services, it is the marketplace of ideas challenging tyranny and championing democracy. It has made lies harder to sustain, information harder to repress and injustice harder to ignore.

But while the Internet has become a dependable part of our lives, it is essential that we not take it for granted or make assumptions about a medium that is still taking shape and that few in Congress fully understand.

Moreover, it is important to remember that the Internet we know did not happen by accident. Rather, it grew from a set of principles that we deliberately put into law during a situation not unlike the one before the committee today.

Over 15 years ago, when Congress first started thinking about Internet regulation the concern was protecting children from pornography. There were competing ideas and some argued that Congress should simply censor the Internet and use the government to cut off access to objectionable material.

But a few of us saw value in letting the Internet develop free from corporate or government control. Instead of having government censor the web, we developed an approach that would empower users and technology to address content concerns on their own. And we took the opportunity to pass a law that said that neutral parties on the net are not liable for the actions of bad actors.

That fundamental principle enshrined in Section 230 of the Communications Decency Act both addressed the problem and freed innovators to develop new ideas like YouTube, Facebook, Wikipedia and Twitter. So now, as we again debate web censorship, let's ask ourselves: What next generation of innovations won't be realized if we backtrack on that principal now?

Yes, the Internet needs reasonable laws and bad actors need to be pursued, but the freedoms of billions of individual Internet users should not be sacrificed in the interest of easing that pursuit. The decisions we make to police the Internet today will also govern how this relatively new medium will continue to develop and shape our world. And yes, giving moneyed interests a louder voice and a greater ability to determine what that online world will look like would fundamentally alter the Internet which currently treats all voices as equal.

As I have said before, this is not an issue where we should use a bunker-buster bomb when a laser beam would do. And that is not just my opinion, venture capitalists who fund Internet start-ups, the biggest and smallest actors in the tech community, law professors concerned with speech, Internet technologists, security experts and mainstream and new media have all expressed concerns about the legislation advancing in Congress.

In writing laws to police the Internet, we need to consider more than how effective a proposed remedy would be at combating infringement, we must also consider the impact proposed remedies will have on everything else online. This means keeping the following in mind:

1. Be deliberate. While rights holders and law enforcement are understandably eager to go after bad actors, we must be mindful of the precedents we set here at home, and around the world.
2. Get the scope right. Narrowly focus law enforcement's authority on those who are willfully and deliberately breaking the law or infringing on others' property rights for commercial gain.
3. Avoid collateral damage. Rather than frustrating the architecture of the Internet or establishing a censoring regime, consider instead promoting approaches that empower users and do no harm to the 'Net. More simply, fish for tuna without catching dolphins.
4. Promote innovation over litigation. Our efforts should be to protect copyrights and trademarks, not outdated business models.

Again, I thank the committee for its consideration of my views.

Prepared Statement of Terry Hart, Creator of Copyhype

Statement of Terry Hart on H.R. 3261, the "Stop Online Piracy Act"

House Judiciary Committee

November 11, 2011

My name is Terry Hart, and I am the creator of Copyhype, a blog devoted to reasoned analysis of copyright issues in a digital age. Since August of 2010, I have written over 200,000 words on the subject, receiving positive attention from many within the copyright community. I am writing today in support of the recently introduced Stop Online Piracy Act (H.R. 3261).

I am passionate about the framework provided by copyright law because I am passionate about the expressive works that have been created in the US over the past 200 plus years because of this framework. From the silly to the sublime, to those that educate and those that entertain, these works have advanced our society, our culture, and our economy. As a media and cultural consumer, I am excited by the increasingly innovative new ways I can access the news, movies, television shows, music, and other works I love online, and I strongly hope that those who create them can continue to create.

I am pleased the House Judiciary Committee has recently introduced the Stop Online Piracy Act. I believe this legislation is both necessary and carefully crafted to ensure creators have effective recourse against sites that profit off misappropriation of their work.

The bill features many important provisions, provisions concerning the denial of US capital to notorious foreign infringers and trafficking in inherently dangerous goods and services, for example, but I will limit my remarks to Sections 102 and 103, which specifically address the problem of online, commercial piracy.

Effective copyright protection, on a fundamental level, is a significant governmental interest, and one of the few enumerated powers of the federal government in the Constitution. In 1832, the Supreme Court said "To promote the progress of the useful arts is the interest and policy of every enlightened government." *Grant v. Raymond,* 31 US 218. Only two years later,

Supreme Court Justice Thompson said in his dissent to the seminal opinion in *Wheaton v. Peters*, "In my judgment, every principle of justice, equity, morality, fitness and sound policy concurs, in protecting the literary labours of men, to the same extent that property acquired by manual labour is protected." 33 US 591 (1834).

The history of copyright law presents a common theme of technological advancement bringing challenges to creators. In the past, we've seen these challenges with the introduction of new forms of media that allowed the recording of sound, images, and motion pictures; broadcasting in the form of radio and television; and even advancements in transportation that have made our world smaller and more connected. Today, creators face challenges to adapt to digital technologies and the Internet, which allows global communication on an unprecedented scale.

But no matter how rapidly technology advances, we should not lose sight of the fundamental principles of "justice, equity, morality, fitness and sound policy" that the protection of expression is built on.

In the words of James Madison, "The public good fully coincides" with "the claims of individuals" under copyright law. *Federalist papers*, No. 43. The introduction of new expressive works, whether in the form of books, music, films, television, photographs, do much to advance this public good. They teach, entertain, and shed light on the human condition. So it is vitally important that those works are protected just as much online as they are offline.

The Internet today looks vastly different today than it did in 1998, when the Digital Millennium Copyright Act was enacted. There was no Google, no YouTube, and no Facebook. The technologies that make rich, fully-interactive sites like these possible simply didn't exist at the time. It would be hard to imagine a world wide web like this today. Today's web allows a myriad of ways for people to engage in communication, commerce, social networking, entertainment, and learning. This is possible because the technology behind the web continued to progress, rather than being frozen in place. The same should be true of copyright law.

The consensus is that the DMCA has generally worked well for copyright holders and service providers. Its safe harbors shield service providers from liability for material uploaded by users where the service provider doesn't have knowledge that the material is infringing, doesn't receive a direct financial benefit from the infringing activity where the provider has the right and ability to control the activity, and acts expeditiously to disable access to uploaded material when it receives a notification of claimed infringement. These notice-and-takedown provisions can be more effective and efficient for removing infringing material than litigation. They work well, in other words, for good faith, legitimate service providers who cooperate with copyright holders to detect and deal with online infringement.

They should not, however, provide cover for service providers who deliberately set out to build sites based on infringement -- where, for example, the site was primarily designed to have no other purpose than to engage in or facilitate infringing acts, the site operator has taken deliberate action to remain unaware of a high probability that the site is used for infringement, or the site operator has taken affirmative steps to promote the use of the site for infringing acts.

The DMCA safe harbors were crafted to provide legal certainty in the new online world and protect service providers from the risk of liability for inadvertent or incidental infringement that they aren't aware of or can't monitor or control. They certainly weren't crafted to protect against those who actively and deliberately design and operate their sites to profit off piracy.

In practice, the DMCA notice-and-takedown provisions are ineffective against sites like this. Many creators would find it a full time job to send notices against these types of sites. And the provisions are especially ineffective against sites that are directed at and easily accessible by US residents but located outside the US and dismissive of US law.

Sections 102 and 103 of the Stop Online Piracy Act fill this gap by giving the Attorney General and copyright holders new tools that directly target rogue sites. The goal of this legislation is not to completely eradicate online piracy, or allow copyright owners to "go back to the way things were." Piracy is inherently part of the copyright landscape, and it will always exist in some form or another.

The goal is rather to allow creators and legitimate intermediaries to continue to develop sustainable business models that allow both widespread dissemination of content and the ability to be remunerated for investing time and money creating that content. Obviously, one of the big challenges facing creators is figuring out these business models, but that doesn't mean the law shouldn't also play a role.

Nearly forty years ago, former Register of Copyrights Barbara Ringer delivered an essay at a time when Congress was in the midst of reforming the Copyright Act to ensure it would remain relevant in the information age. Like today, it was a time of rapid technological change, with new stakeholders emerging and contentious debate. But though the technologies and players were different, Ringer's words remain just as relevant today:

> "If the copyright law is to continue to function on the side of light against darkness, good against evil, truth against newspeak, it must broaden its base and its goals. Freedom of speech and freedom of the press are meaningless unless authors are able to create independently from control by anyone, and to find a way to put their works before the public. Economic advantage and the shibboleth of "convenience" distort the copyright law into a weapon against authors. Anyone who cares about freedom and authorship must insure that, in the process of improving the efficiency of our law, we do not throw it all the way back to its repressive origins in the Middle Ages." (Barbara Ringer, *Demonology of Copyright* (1974).)

Critics of the Stop Online Piracy Act have raised concerns about the First Amendment and due process implications of the bill, which I will look at in more detail.

Copyright Law and Freedom of Expression

The introduction of the Stop Online Piracy Act has raised free speech concerns from various parties. It's absolutely vital that the proposed bill -- *any* bill for that matter -- conforms with the First Amendment, which, I believe, it does. Noted First Amendment expert Floyd Abrams believes the bill is fully compatible with First Amendment protections as well, as he explained in a recent letter sent to this Committee.

But it's also important to keep in mind that copyright law itself serves an important role in furthering the goals of freedom of expression. This role has been recognized since the founding

of the United States. As the Supreme Court said in *Eldred v. Ashcroft*, "the Framers intended copyright itself to be the engine of free expression."

Founding Father and second president John Adams once wrote, "Property must be secured, or liberty cannot exist." Our third president, and the Father of the Constitution, James Madison added, "The advancement and diffusion of knowledge is the only guardian of true liberty."

The Copyright Clause in the Constitution incorporates these ideas, thus serving as a critical component in the protection of liberty. It gives Congress the power to secure to authors the exclusive rights in their writings in order to promote the progress of the useful arts and sciences. The importance of this power cannot be understated, and neither can the importance that these exclusive rights be truly *secure* in order to promote progress and spur diffusion of new expression.

That copyright law complements rather than conflicts with freedom of expression has been recognized many times since then. In an 1844 article appearing in *The Reasoner* magazine, the author writes: "If the public desire a really free press, they must not look to it as a source of taxation; and if they are anxious for truth, for elevated and elevating sentiments, for ideas matured by study and reflection, and an honest exposition of grievances, they must recognise original articles as property, and secure them against a plundering appropriation by a copyright." And in an 1880 treatise on the liberty of the press, the author characterizes the "valuable property in the hands of the author who composes and publishes his thoughts" as one of the forms "which the right of free speech and thought assumes."

Perhaps the best examination of the complementary relationship between copyright and freedom of expression comes from former Register of Copyrights Barbara Ringer, who noted:

> "[I]t is important to recognize that the Statute of Anne of 1710, the first copyright statute anywhere and the Mother of us all, was enacted precisely because the whole autocratic censorship/monopoly/ licensing apparatus had broken down completely. As a result of the bloodless revolution taking place in the English constitutional system, basic individual freedoms, notably freedom of speech and freedom of the press, were becoming established under common law principles. The Statute of Anne marked the end of autocracy in English copyright and established a set of democratic principles : recognition of the individual

> author as the ultimate beneficiary and fountainhead of protection and a guarantee of legal protection against unauthorized use for limited times, without any elements of prior restraint of censorship by government or its agents."

She later observes, "It is striking that the second and third copyright statutes in the world — those of the United States of America and of France — were adopted immediately following the revolutions in those countries that overthrew autocratic government and were based on ideals of personal liberty and individual freedom."

Prior restraint and censorship are antithetical to the First Amendment, but doing nothing in the face of rampant online piracy disgraces the goals of freedom of expression as well. The Stop Online Piracy Act helps secure creators' rights online. Rogue sites jeopardize the ability of creators and firms to invest time and resources into creating new expression that advances society and culture. Current law is insufficient to address this harm; this bill would help restore the security of copyrights online.

The Procedure of Sections 102 and 103 of the Stop Online Piracy Act

The rule of law is one of the most central and vital aspects of a free society. The US Constitution guarantees fair and impartial proceedings, protects citizens from arbitrary and unequal applications of law, and limits what the government can do before depriving someone of life, liberty, or property.

But like freedom of speech, the concept of due process encompasses more than just Constitutional limits. Due process requires that rights have effective remedies available. Doing nothing violates the spirit of the rule of law.

The Stop Online Piracy Act strikes the correct balance between giving copyright holders an effective process for addressing sites whose only purpose is profiting off of the misappropriation of their works and ensuring that legitimate site operators are not punished. A closer look at the procedures laid out in Sections 102 and 103 of the bill shows this balance.

Section 102 of the bill provides for an action by the Attorney General against foreign infringing sites. Like any other civil suit, such an action would begin with a complaint filed in

federal court and notice given to the defendant, who may then defend against the suit as any civil defendant may.

The Attorney General is then directed to move for an injunction against the site operator "to cease and desist from undertaking any further activity as a foreign infringing site." These injunctions are governed by the same Federal Rules of Civil Procedure as any civil injunction, and would not issue until a court determination made after both sides are heard.1

From there, the Attorney General can seek court orders against service providers that provide access to the foreign infringing site, Internet search engines that provide links to the site based on a user query or selection, payment network providers that process or complete financial transactions for the site, and Internet advertising services that contract to provide advertising to or for the site. These four service providers are only required to take "technically feasible and reasonable measures" to comply with these orders.

The bill limits what the Attorney General can do to ensure compliance with these orders to injunctive relief against a service provider that "knowingly and willingly" fails to comply with the order. The bill provides an affirmative defense for a service provider in the event it "does not have the technical means to comply with this subsection without incurring an unreasonable economic burden."

In addition, at any time after a court order is issued under this section, the foreign infringing site or any service provider served with an order may petition to modify, suspend, or vacate the order if the "foreign Internet site subject to the order is no longer, or never was, a foreign infringing site" or, more broadly, if "the interests of justice otherwise require" modifying, suspending, or vacating the order. It should also be noted that under this portion of the bill, any service provider subject to a court order may intervene at any time in any action.

Taken together, these provisions provide for robust procedural protections that fully comport with due process of law under the Constitution. It would not be likely or easy to abuse the provisions of Section 102 of the Stop Online Piracy Act.

---

1 Except in the case of a temporary restraining order, which may be made *ex parte*.

Section 103 of the Stop Online Piracy Act provides for a notice procedure similar to the one found in the DMCA. A copyright owner may serve notice on a payment network provider or Internet advertising provider that provides services to a site "dedicated to theft of U.S. property." The bill defines such a site as one that , in part, "is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in, offering goods or services in a manner that engages in, enables, or facilitates" copyright infringement; the operator "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of" the site to carry out infringing acts; or the site is operated "with the object of promoting ... its use to carry out acts that constitute" copyright infringement, "as shown by clear expression or other affirmative steps taken to foster infringement."

These definitions are drawn directly from existing Supreme Court precedent that establishes secondary liability for copyright infringement and would not diminish or upend existing DMCA safe harbors for good faith, legitimate service providers.

Should a service provider fail to comply with a notice, or should a site serve a counter-notification under the bill, nothing happens unless and until a copyright owner files a suit in court. This action mirrors the one available to the Attorney General in Section 102 in the bill, except the court orders are limited to only payment network and Internet advertising providers. As in that action, the procedural protections available to all parties involved are robust.

Finally, Section 103 provides penalties to protect against copyright owners using the notice procedure in bad faith. These penalties are the same as those available under the DMCA, which holds that a content owner who "knowingly materially misrepresents" that content is infringing is liable for any damages, attorney fees, and costs incurred by the user as a result of the content being taken down. But while the language of the Stop Online Piracy Act mirrors that in the DMCA, there are two practical realities that make it different.

First, a good faith effort to determine that an entire site is "dedicated to theft of US property" under the definition of the bill requires considerably more effort than determining whether a single file is infringing. The notification itself requires substantially more investigation

than a DMCA notice. Under the DMCA, a copyright owner need only identify what work is being infringed and the content that is infringing. Under the Stop Online Piracy Act, the copyright owner must show, among other things, "specific facts to support the claim that the Internet site, or portion thereof, is dedicated to theft of U.S. property" and "clearly show that immediate and irreparable injury, loss, or damage will result" to the copyright owner in the absence of timely action; "Information reasonably sufficient to establish that the payment network provider or Internet advertising service is providing payment processing or Internet advertising services for such site"; and identification of evidence that indicates the site is US-directed.

Second, the risk of making a material misrepresentation is much higher. The operator of a site whose sources of income have been threatened is far likelier to push back than a user whose video was taken down. And unlike the nominal damages present in a DMCA takedown, the loss of ad revenues and credit card transactions because of a bad faith takedown could add up.

Conclusion

Sections 102 and 103 of the Stop Online Piracy Act represent a good start for creators who have long noted the injustice of others profiting from online piracy and escaping liability. Web services who are acting legitimately and legally should welcome rogue sites legislation because effective protection of creative labor is vital to a functioning online marketplace, and a functioning online marketplace benefits us all. With this bill Congress can truly secure the exclusive rights of creators. Doing so not only protects creators but also ensures that the development of innovative and sustainable services for consumers to access and enjoy media and content can continue.

List of submitters contributing material in association with the consideration of H.R. 3261*

60 plus
ABC
AFL-CIO
Alliance for Safe Online Pharmacies
American Bankers Association
American Civil Liberties Union
American Consumer Institute Center for Citizen Research
American Society of Composers, Authors and Publishers
Americans for Tax Reform
Association of American Publishers
Association of State Criminal Investigative Agencies
Association of Talent Agents
Beachbody, LLC
BMG Chrysalis
Broadcast Music Incorporated
Building and Construction Trades Department (AFL-CIO)
Capitol Records Nashville
CBS (including subsidiary Simon & Schuster)
Cengage Learning
Center for Indicvidual Freedom
Christian Music Trade Association
Church Music Publishers' Association
Coalition Against Online Video Piracy
Comcast/NBCUniversal
Computer & Communications Industry Association
Concerned Women for America
Congressional Fire Services Institute
Copyright Alliance
Coty, Inc.
Council of Better Business Bureaus
Council of State Governments
Country Music Association
Country Music Television
Creative Community
Deluxe Entertainment Services Group, Inc.
Disney Publishing Worldwide, Inc.
Educause
Electronic Transactions Association
Elsevier
EMI Christian Music Group
EMI Music Publishing
Entertainment Software Association
ESPN
GoDaddy
Gospel Music Association
Graphic Artists Guild
Hachette Book Group
HarperCollins Publishers Worldwide, Inc.
Hyperion
Independent Film & Television Alliance
International Anti-Counterfeiting Coalition
International Brotherhood of Electrical Workers
International Brotherhood of Teamsters
International Trademark Association

*The material received by the Subcommittee from the submitters whose names appear in this list, is not printed in this hearing record but is on file with the Subcommittee.

International Union of Police Associations
Internet Society
Joint letter of support from AFM, AFTRA, DGA, IATSE, IBT, and SAG
Joint letter of opposition from ALA, ARL, CDT, CEI, DP,EFF, FH,HRF, HRW, Internews, NAFOTI, PK and TF
Joint letter of opposition from educational interests
Joint letter of support from First Amendment & Intellectual Property Counsels
Let Freedom Ring
Library Copyright Alliance
Lilly
L'Oreal
Lost Highway Records
Macmilian
Major City Chiefs
Major County Sheriffs
Major League Baseball
Marvel Entertainment, LLC
Mastercard Worldwide
MCA Records
McGraw-Hill Education
Mercury Nashville
Minor League Baseball
Minority Media & Telecom Council
Motion Picture Association of America
Moving Picture Technicians
MPA—The Association of Magazine Media
National Association of Fusion Center Directors
National Association of Manufacturers
National Association of Prosecutor Coordinators
National Association of Theater Owners
National Association of State Chief Information Officers
National Cable & Telecommunications Association
National Center for Victims of Crime
National Criminal Justice Association
National District Attorneys Association
National Domestic Preparedness Coalition
National Football League
National Governors Association
National League of Cities
National Narcotics Officers' Association Coalition
National Sheriffs Association
National Songwriters Association
National Troopers Coalition
Net Coalition
News Corporation
Pearson Education
Penguin Group (USA), Inc.
Pfizer, Inc.
Pharmaceutical Research and Manufacturers of America
Professors' Letter In Opposition to PROTECT-IP
Provident Music Group
Random House
Raulet Property Partners
Republic Nashville
Revlon
Sandia National Laboratories
Scholastic, Inc.
Showdog Universal Music
Sony Music Entertainment
Sony Music Nashville

Sony/ATV Music Publishing
State International Development Organizations
The Estee Lauder Companies
The Honorable Ron Wyden
The Perseus Books Group
Tiffany and Co.
Time Warner
True Religion
U.S. Chamber of Commerce
U.S. Conference of Mayors
U.S. Olympic Committee
Ultimate Fighting Championship
UMG Publishing Group Nashville
United States Tennis Association
Universal Music
Universal Music Publishing Group
Viacom
Visa Inc.
W.W. Norton & Company
Wallace Bajjali Development Partners LP
Warner Music Group
Warner Music Nashville
Wolters Kluewer Health
Word Entertainment
Zumba Fitness