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

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

July 5, 2011

To Members of the United States Congress:

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

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

The Act goes still further. It requires credit card providers, advertisers, and search engines to refuse to deal with the owners of such sites. For example, search engines are required to "(i) remove or disable access to the Internet site associated with

the domain name set forth in the court order; or (ii) not serve a hypertext link to such Internet site." In the case of credit card companies and advertisers, they must stop doing business not only with sites the government has chosen to sue but any site that a private copyright or trademark owner claims is predominantly infringing. Giving this enormous new power not just to the government but to any copyright and trademark owner would not only disrupt the operations of the allegedly infringing web site without a final judgment of wrongdoing, but would make it extraordinarily difficult for advertisers and credit card companies to do business on the Internet.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signed,[7]

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

Professor Brook K. Baker
Northeastern University School of Law

Professor Derek E. Bambauer
Brooklyn Law School

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

Professor Mark Bartholomew
University at Buffalo Law School

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

Professor Ann M. Bartow
Pace Law School

Professor Marsha Baum
University of New Mexico School of Law

Professor Yochai Benkler
Harvard Law School

Professor Oren Bracha
University of Texas School of Law

Professor Annemarie Bridy
University of Idaho College of Law

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

Professor Irene Calboli
Marquette University School of Law

Professor Adam Candeub
Michigan State University College of Law

Professor Michael Carrier
Rutgers Law School – Camden

Professor Michael W. Carroll
Washington College of Law
American University

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

Professor Anupam Chander
University of California-Davis School of Law

Professor Andrew Chin
University of North Carolina School of Law

Professor Ralph D. Clifford
University of Massachusetts School of Law

Professor Julie E. Cohen
Georgetown University Law Center

Professor G. Marcus Cole
Stanford Law School

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

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

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

Professor Christopher A. Cotropia
University of Richmond School of Law

Professor Thomas Cotter
University of Minnesota School of Law

Professor Julie Cromer Young
Thomas Jefferson School of Law

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

Professor Eric B. Easton
University of Baltimore School of Law

Anthony Falzone
Director, Fair Use Project
Stanford Law School

Professor Nita Farahany
Vanderbilt Law School

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

Professor Sean Flynn
Washington College of Law
American University

Professor Brett M. Frischmann
Cardozo Law School
Yeshiva University

Professor Jeanne C. Fromer
Fordham Law School

Professor William T. Gallagher
Golden Gate University School of Law

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

Professor Deborah Gerhardt
University of North Carolina School of Law

Professor Llew Gibbons
University of Toledo College of Law

Professor Eric Goldman
Santa Clara University School of Law

Professor Marc Greenberg
Golden Gate University School of Law

Professor James Grimmelman
New York Law School

Professor Leah Chan Grinvald
St. Louis University School of Law

Professor Richard Gruner
John Marshall Law School

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

Professor Robert A. Heverly
Albany Law School
Union University

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

Professor Herbert Hovenkamp
University of Iowa College of Law

Professor Dan Hunter

New York Law School

Professor David R. Johnson
New York Law School

Professor Faye E. Jones
Florida State University College of Law

Professor Amy Kapczynski
University of California-Berkeley Law School

Professor Dennis S. Karjala
Arizona State University College of Law

Professor Anne Klinefelter
University of North Carolina College of Law

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

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

Professor Mark Lemley
Stanford Law School

Professor Lawrence Lessig
Harvard Law School

Professor David S. Levine
Elon University School of Law

Professor Yvette Joy Liebesman
St. Louis University School of Law

Professor Lydia Pallas Loren
Lewis & Clark Law School

Professor Michael J. Madison
University of Pittsburgh School of Law

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

Professor Phil Malone
Harvard Law School

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

Professor Jonathan Masur
University of Chicago Law School

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

Professor William McGeveran
University of Minnesota Law School

Professor Stephen McJohn
Suffolk University Law School

Professor Mark P. McKenna
Notre Dame Law School

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

Professor Viva Moffat
University of Denver College of Law

Professor Ira Nathenson
St. Thomas University School of Law

Professor Tyler T. Ochoa
Santa Clara University School of Law

Professor David S. Olson
Boston College Law School

Professor Barak Y. Orbach
University of Arizona College of Law

Professor Kristen Osenga
University of Richmond School of Law

Professor Aaron Perzanowski

Wayne State University Law School

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

Professor David G. Post
Temple University School of Law

Professor Connie Davis Powell
Baylor University School of Law

Professor Margaret Jane Radin
University of Michigan Law School

Professor Glenn Reynolds
University of Tennessee Law School

Professor David A. Rice
Roger Williams University School of Law

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

Professor Michael Risch
Villanova Law School

Professor Betsy Rosenblatt
Whittier Law School

Professor Matthew Sag
Loyola University-Chicago School of Law

Professor Pamela Samuelson
University of California-Berkeley Law School

Professor Sharon K. Sandeen
Hamline University School of Law

Professor Jason M. Schultz
UC Berkeley Law School

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

Professor Jessica Silbey
Suffolk University Law School

Professor Brenda M. Simon
Thomas Jefferson School of Law

Professor David E. Sorkin
John Marshall Law School

Professor Christopher Jon Sprigman
University of Virginia School of Law

Professor Katherine J. Strandburg
NYU Law School

Professor Madhavi Sunder
University of California-Davis School of Law

Professor Rebecca Tushnet
Georgetown University Law Center

Professor Deborah Tussey
Oklahoma City University School of Law

Professor Barbara van Schewick
Stanford Law School

Professor Eugene Volokh
UCLA School of Law

Professor Sarah K. Wiant
William & Mary Law School

Professor Darryl C. Wilson
Stetson University College of Law

Professor Jane K. Winn
University of Washington School of Law

Professor Peter K. Yu
Drake University Law School

Professor Tim Zick
William & Mary Law School