



KEEPING THE INTERNET  
OPEN • INNOVATIVE • FREE

[www.cdt.org](http://www.cdt.org)

CENTER FOR DEMOCRACY  
& TECHNOLOGY

1634 I Street, NW  
Suite 1100  
Washington, DC 20006

P +1-202-637-9800

F +1-202-637-0968

E [info@cdt.org](mailto:info@cdt.org)

## THE DANGERS OF S. 3804: DOMAIN NAME SEIZURES AND BLOCKING POSE THREATS TO FREE EXPRESSION, GLOBAL INTERNET FREEDOM, AND THE INTERNET'S OPEN ARCHITECTURE

September 28, 2010

Copyright infringement is a serious problem, and CDT harbors no sympathy for websites whose primary purpose is to enable widespread violation of copyright and other intellectual property rights. But methods embraced by S. 3804, the “Combating Online Infringement and Counterfeits Act,” would mark a sea change in U.S. policy towards the Internet. In particular, U.S. government action to seize domain names and to direct Internet Service Providers (ISPs) to block government-blacklisted sites would set dangerous precedents with serious consequences for free expression, global Internet freedom, and the Internet’s open and global architecture. If enacted, the bill would be a significant step towards the balkanization of the Internet. These consequences are much too significant to address in a rushed fashion in the waning hours of the 111th Congress.

S. 3804 raises major problems in the following areas.

### 1. Free Expression

S. 3804 raises serious First Amendment concerns, in at least three distinct ways. First, it directs courts to impose “prior restraints” on speech, which are “the most serious and the least tolerable infringement on First Amendment rights.”<sup>1</sup> Our Constitution strongly counsels against prior restraints that block access to speech, even if the speech might later be proven to be unlawful. The First Amendment teaches that speech should be pro-actively blocked only in the rarest of circumstances.<sup>2</sup> This is especially true because the type of restraint imposed by S. 3804 – the total suspension or blocking of a site’s domain name – would unavoidably block lawful content as well as infringing content. Even a site that is deemed to be “primarily designed” to offer infringing content under the bill’s vague definition is almost certain to also contain at least some non-infringing content, which is fully protected by the First Amendment. The First Amendment requires that an order against speech “be precise and narrowly tailored to

---

<sup>1</sup> *Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). See also *Center For Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004) (holding that statute requiring the blocking of access to particular domain names and IP addresses amounted to an unconstitutional prior restraint).

<sup>2</sup> See *Near v. Minnesota*, 283 U.S. 697 (1931).

achieve the pin-pointed objective of the needs of the case.”<sup>3</sup> It does not permit the type of broad censorship of speech required by S. 3804.

Second, S. 3804 provides inadequate procedural protections to accompany its restrictions on speech. The Supreme Court, in *Freedman v. Maryland* and its progeny,<sup>4</sup> has made clear that a prior restraint (if permitted at all) must be coupled with very strong procedural safeguards, which S. 3804 lacks.<sup>5</sup> “The separation of legitimate speech from the illegitimate calls for . . . sensitive tools”<sup>6</sup> and due process considerations demand that a prior restraint only be enforced following a full, adversarial hearing on the merits of the case. This bill, however, permits the Attorney General to seek injunctive relief, including temporary restraining orders, and to extend the courts’ reach to domain names owned by speakers far outside the United State’s geographic borders – far from the kind of procedure that ensures a full and fair trial with all interested parties present.<sup>7</sup> S. 3804 also permits modification of the court’s order to block additional domains based on an assertion of common ownership, without even the inadequate substantive and procedural requirements contained elsewhere in the bill. With no provision for an adversarial hearing on the merits for distinct domain names, S. 3804 justifies the censorship of speech based on the identity of the speaker, something the Constitution cannot tolerate.

In addition to the seizure and blocking of domain names, S. 3804 commands the Attorney General to publish a blacklist of domain names that the Department of Justice “reasonably believes” are dedicated to infringing activities. ISPs, registrars, and registries are encouraged (and granted the same immunity they would receive for actions taken pursuant to a court order) to block these domain names. This scheme – closely analogous to the informal blacklist held to be unconstitutional in *Bantam Books v. Sullivan*<sup>9</sup> – encourages blocking of domains without providing *any* of the procedural safeguards the Constitution requires. Moreover, S. 3804 places the onus for appealing this block on the domain name owner, not on the government, where it belongs.<sup>10</sup> And, while the courts have been clear that prior restraints on speech must be limited to “the shortest fixed period compatible with sound judicial resolution,”<sup>11</sup> this bill requires domain name owners to petition the AG for removal of the domain name from the blacklist (via an as-yet-unspecified procedure) and only then provides the owner with the opportunity for judicial review. This process completely fails to meet the Constitutional requirement that such a law

---

<sup>3</sup> *Tory v. Cochran*, 544 U.S. 734, 736 (2005) (internal quotes omitted).

<sup>4</sup> *Freedman v. Maryland*, 380 U.S. 51 (1965); see also *United States v. Thirty-Seven Photographs*, 402 U.S. 363 (1971); *Southeastern Promotions v. Conrad*, 420 U.S. 546 (1975).

<sup>5</sup> See also *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (striking down Internet blocking law on numerous grounds, including inadequate procedural protections).

<sup>6</sup> *Speiser v. Randall*, 357 U.S. 513, 525 (1958).

<sup>7</sup> The few cases in which a system of prior restraints on speech have satisfied the First Amendment’s stringent requirements, there has been little doubt that the publisher of the contested material was able to appear in court to defend the material. See, e.g., *Kingsley v. Brown*, 354 U.S. 436 (1957). But S. 3804, with its dramatic assertion of global jurisdiction and anemic provisions for giving notice to the owner of a challenged domain, does not guarantee the same level of process.

<sup>9</sup> *Bantam Books v. Sullivan*, 372 U.S. 58 (1962). See also *Ctr. For Democracy & Tech, v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (striking down informal blacklist of sites).

<sup>10</sup> “[T]he burden of instituting judicial proceedings, and of proving that the material is unprotected, must rest on the censor.” *Southeastern Promotions, Ltd. v. Conrad*, 402 U.S. 546, 560 (1975).

<sup>11</sup> *Freedman v. Maryland*, 380 U.S. 51, 58 (1965); see also *United States v. Thirty-seven Photographs*, 402 U.S. 363, 367 (1971).

“assure[s] a prompt final judicial decision to minimize the impact of possibly erroneous administrative action.”<sup>13</sup>

Beyond these unconstitutional threats to free speech, S. 3804 also raises significant risk that foreign governments will be able to restrict the speech that is available to American Internet users. As one example, ten years ago France sought to censor content on yahoo.com, hosted in the United States, but it found that it could not reach Yahoo! directly (and the First Amendment would have prevented any effort to impose the censorship through the U.S. courts). But today, France could follow the lead set by S. 3804 (if enacted) and seek to seize the yahoo.com domain name by issuing an order to the operator of the .com registry (which operates DNS servers in France). That operator, Verisign, also runs DNS servers in China, Russia, Brazil, Singapore, and many other countries, leaving .com and .net domains open to blocking orders from a broad range of countries. By setting the precedent that any country can block the world’s access to Internet content based solely on the location of DNS servers, S. 3804 would certainly lead to the reduction of lawful speech available to American Internet users.

## 2. Global Internet Freedom / International Human Rights

Over forty countries (and growing) now filter the Internet to some degree, and even many liberal democracies like Australia are considering mandatory filtering regimes in which the government requires ISPs to block certain websites.<sup>14</sup> Historically, the United States has been the bulwark against censorship and government-imposed blocking of Internet content. If the United States sets the precedent that any country can seize or order the blocking of a domain name if some of the content on the domain (wherever located) violates the country’s local laws, the effort to protect the rights of Internet users, human rights defenders, and citizen journalists to speak and access lawful content online will be critically harmed.

The human rights community has strongly condemned countries that use tactics proposed in S. 3804. For example, Turkey has blocked YouTube for several years because YouTube refuses to disable access to content for the site’s global user base at the government’s request, merely because that content is illegal under local law.<sup>15</sup> While the technical mechanisms may vary, the effect is the same: if enacted, S. 3804 would stand for the proposition that countries have the right to insist on removal of content from the global Internet in service to the exigencies of domestic law—and nothing would limit the application of this approach to copyright infringement.

As noted in the previous section, S. 3804 also would drive many states, including liberal democracies, to adopt similar policies directed at U.S. content, taking it down worldwide. The scope of protection provided by the First Amendment remains the most expansive in the world,

---

<sup>13</sup> *United States v. Thirty-seven Photographs*, 402 U.S. 363, 367 (1971) (internal citations omitted).

<sup>14</sup> In April 2010, the U.S. Ambassador to Australia, Jeff Bleich, commented on the Australian filtering proposal on Australian public TV: “Well, what we’ve said is that we have been able to accomplish the goals that Australia has described, which is to capture and prosecute child pornographers and others who use the internet for terrible purposes, without having to use internet filters.” Transcript of “The American Ambassador on Q&A,” Q&A, ABC TV, <http://www.abc.net.au/tv/qanda/txt/s2864512.htm?show=transcript>. S. 3804 seems to send precisely the opposite signal.

<sup>15</sup> See Jeffrey Rosen, “Google’s Gatekeepers,” *New York Times*, Nov. 28, 2008, <http://www.nytimes.com/2008/11/30/magazine/30google-t.html> (discussing struggle between Google and Turkey over YouTube videos). Advocates in Turkey have been working to challenge this order.

and speech protected in the United States remains proscribable in many other democratic countries (for example, hate speech in France). Local access to such speech remains a frustration for governments in those countries, and they would welcome a U.S.-based precedent to justify blocking it.

In countries where rule of law is weak or entirely absent, meanwhile, S. 3804's approach opens the door to serious misuse. As Microsoft's recent experiences in Russia have revealed, governments can exploit copyright laws as a pretext for suppression of political speech.<sup>16</sup> Further, once the United States sends the green light, the use of domain locking or ISP domain blocking to silence other kinds of content considered unlawful in a given country—from criticism of the monarchy in Thailand to any speech that “harms the interests of the nation” in China—will surely spread, impacting bloggers, citizen journalists, human rights advocates and ordinary users everywhere. The precedent that domain locking or blocking can be encouraged through an extrajudicial blacklist only intensifies this risk. Repressive countries will certainly not limit the application of this approach, and the work of human rights groups will very quickly make its way to these blacklists. If many countries follow the U.S. lead, the result would be a race to the bottom on the global Internet towards the most restrictive speech regimes.

Finally, directing ISPs to block content through DNS tampering directly undermines the U.S. government's commitment to advancing one global Internet. In her February speech at the Newseum, Secretary of State Clinton decried the development of “a new information curtain [] descending across much of the world,” and declared the United States' support “for a single Internet where all of humanity has equal access to knowledge and ideas.”<sup>17</sup> If many other countries adopt S. 3804's approach—and there is little doubt that many would—it will worsen the balkanization of the Internet, undermining the right to freedom of expression and association and threatening the potential of the Internet as a powerful tool for promoting human rights.

### 3. Internet Architecture / Role of ISPs

S. 3804, if enacted, would be the first U.S. statute ever to require ISPs to block certain Internet communications based on their content. This would mark a striking departure from established U.S. law and policy regarding the role of ISPs.

Congress has expressly rejected the notion that ISPs should be required to police user behavior. 47 U.S.C. § 230(c)(1) states that ISPs shall not be treated as the publishers or speakers of their users' communications, while 17 U.S.C. § 512(a) directs that ISPs shall not be liable when users transmit infringing material. These legislative safe harbors reflect a deliberate policy choice – a choice to allow ISPs to focus on empowering communications by and among users without the ISPs monitoring, supervising, or playing any other gatekeeping or policing role.

This policy choice is what has enabled the Internet's uniquely decentralized structure – a structure which in turn has enabled the Internet to serve as an unprecedented platform for innovation, speech, collaboration, civic engagement, and economic growth. Given the lack of central supervision, it is also true that some people inevitably will use the network in connection

---

<sup>16</sup> Clifford J. Levy, “Russia Uses Microsoft to Suppress Dissent,” NY Times, September 11, 2010, <http://www.nytimes.com/2010/09/12/world/europe/12raids.html>.

<sup>17</sup> US Secretary of State Hillary Rodham Clinton, “Remarks on Internet Freedom,” Washington, DC, January 21, 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>.

with unlawful activity – just as some people use the road network or telephone network in connection with unlawful activity. But decentralization is a core attribute of the Internet, and the policy choices that support it have been tremendously successful.

There is no basis for thinking of S. 3804 as just a minor exception to this important policy. Once the precedent has been established, there will be no principled basis for limiting the ISPs' policing role to copyright infringement. There is no shortage of illegal or unsavory content on the Internet, and well-intentioned advocates for various causes will look to ISP domain-name blocking as the new tool for addressing it. In short, once Congress endorses a new policing role for ISPs, that role will surely grow. As ISPs are enlisted for each new policy aim – however appropriate when viewed in isolation – the unsupervised, decentralized Internet will give way to a controlled, ISP-policed medium. This would be a fundamental change in how the Internet works.

In addition, the framework established in S. 3804 could have a substantial impact on the judicial development of secondary liability law. For example, the DoJ “blacklist” could be used to impute knowledge (a factor in both the safe harbors under 47 U.S.C. § 512 and in the test for contributory liability), or an ISP's role in blocking certain domains under the bill could be argued to support the ISP's right and ability to control a website's behavior (a factor in vicarious liability). The end result could be increased liability risk for ISPs, which would give them a strong incentive to assume more control over user behavior – again, a major departure from the Internet's traditional user-driven architecture.

#### **4. Internet Governance / Domain Name System**

A key international issue over the past ten years has been “Internet governance,” with many countries of the world concerned about what they perceive as undue U.S. control over the Internet, particularly because the U.S. continues to have some direct involvement in the management of the Domain Name System (DNS). An important aspect of American foreign policy under both Republican and Democratic administrations has been to reassure the global community that the United States would not abuse its position of oversight over the DNS. The alternative – sought by countries such as China, Brazil, and others – would have oversight of the DNS wrested from the U.S.-created ICANN and given to the International Telecommunications Union (ITU), which is controlled by the world's governments.

S. 3804 significantly aggravates the situation by suggesting to the world that the U.S. does intend to use the historic nature of the DNS (with American companies administering “.com” and other leading top-level domains) to impose American law on the global Internet. Under the bill, the U.S. asserts that it can take down websites created and operated anywhere in the world, simply based on the fact that the websites use the most popular global top-level domain (.com). This type of assertion of global control is the kind of U.S. exercise of power about which other countries of the world have worried – and about which U.S. foreign policy has sought to reassure the world. Thus S. 3804 directly harms the United States' Internet governance agenda pursued through diplomatic channels over the past ten years.

## 5. Ineffectiveness and Security Risks from Evasion

For all the risks it poses, the domain name blocking contemplated in S. 3804 can be easily circumvented, and thus will have little ultimate effect on online piracy.<sup>18</sup>

The domain name system performs a relatively simple function: translating text URLs into machine-readable IP addresses. While most users rely on their own ISP's DNS server to perform this translation function, this is far from the only option. Users could enter IP addresses manually into their browsers and bookmark those addresses, bypassing the DNS system entirely. Alternatively, since most operating systems come with DNS server functionality built in, users could set up local DNS servers on their own computers, thus avoiding any DNS servers that have been ordered to block. Or operators of blacklisted websites could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers.

In addition, third-party public DNS servers are widely available, and more would inevitably spring up outside the United States to avoid being subject to blocking orders. For Internet users, pointing DNS requests to these unfiltered servers would be simply a matter of updating a single parameter in their operating systems' Internet settings. Users who want to engage in infringement will thus easily be able to route their traffic around DNS providers that enforce the blacklist.

Driving DNS requests to such foreign servers is a very real possibility, and one that could lead to serious unintended consequences for cybersecurity. Once a DNS server set up to circumvent S. 3804 has a large base of regular users, the operator may well be tempted to take advantage of that traffic. It would be easy for that operator to, for example, re-route requests for banking websites not to the requested sites but to phishing sites set up specifically to steal unsuspecting users' personal information in order to gain access to financial accounts or perpetrate other fraud. Though they may be unaware of it, users place an enormous amount of trust in their DNS provider to route requests to the proper sites. ISPs have incentive to maintain that trust, but other DNS operators – especially those with an interest in evading the blocking of sites dedicated to commercial infringement – will likely not share that same incentive. By creating strong incentives to rely on potentially untrustworthy DNS providers, S. 3804 will create a new and very dangerous opportunity for security risks and crime online.

\* \* \*

At a minimum, policy questions of this breadth and magnitude require careful consideration. Concern over copyright infringement is legitimate, but Congress should not take the step of enacting S. 3804 without fully exploring its full potential impact on other core U.S values and policy objectives.

---

<sup>18</sup> This lack of effectiveness speaks directly to S. 3804's unconstitutionality. See, e.g., *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 564 (1980) (law that restricts speech "may not be sustained if it provides only ineffective or remote support for the government's purpose.").