TAKING THE WIND OUT OF THE MOVIE PIRATES' SAILS: THE CONSTITUTIONALITY OF SENATE BILL 3804

Shelly Rosenfeld*

* LL.M., UCLA Law School, 2011; J.D., University of California, Hastings College of the Law, 2010; Masters of Science in Journalism, Northwestern University, 2004; Bachelor of Arts, Political Science, Mass Communications, University of California, Berkeley, 2003. I would like to thank Professor Ken Ziffren for his support through the entire process, and for imparting his wisdom in entertainment law and on the subject of film piracy on the web.

I. INTRODUCTION

> If enacted, [Senate Bill 3804] would be a significant step towards the balkanization of the Internet.[1]
>
> -Center for Democracy and Technology, in a September 2010 Press Release

> I hear periodically, 'Well, Tom Cruise has enough money' or 'Tom Hanks has enough money'False I would say to movie lovers, stick around and watch all of the credits. When you see hundreds of names scrolling across the screen, those are the people whose talents contributed to making that movie, and they need to make a living.[2]
>
> -John Malcolm, former director of worldwide anti-piracy operations for the Motion Picture Association of America

It is precisely the tension between constitutional guarantees and movie piracy's financial impact on the entertainment industry's efforts which forms the basis of a pressing need to explore governmental protections to combat infringing content on the web. The issue of film piracy on the internet has a very wide scope. Because of its global reach, film piracy carries a very large price tag. In fact, worldwide piracy costs United States based companies billions of dollars every year.[3] On November 18, 2010, the Senate Judiciary Committee unanimously approved the "Combating Online Infringement and Counterfeits Act," or COICA.[4] However, while the Bill passed the Senate Judiciary Committee, the Senate did not pass the Bill. Instead, the Bill was rewritten as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property, or Protect IP

---

[1] *Dangers of S.3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Sep. 28, 2010), http://www.cdt.org/report/dangers-s3804-domain-name-seizures-and-blocking-pose-threats-free-expression-global-internet-.

[2] Lisa Respers France, *In Digital Age, Can Movie Piracy Be Stopped?*, CNN (May 1, 2009), http://articles.cnn.com/2009-05-01/tech/wolverine.movie.piracy_1_digital-piracy-digital-age-watermarks?_s=PM:TECH.

[3] Mark Eddington & Antonia Ferrier, *Hatch, International Anti-Piracy Caucus Unveils "2010 International Piracy Watch List"* (May 19, 2010), http://hatch.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=b109414b-1b78-be3e-e0b8-34869d0477c4&Month=5&Year=2010.

[4] John Eggerton, *Judiciary Passes Online Piracy Protection Bill*, BROADCASTING & CABLE (Nov. 18, 2010), http://www.broadcastingcable.com/article/460066-Judiciary_Passes_Online_Piracy_Protection_Bill.php.

Act.[5] Senator Leahy introduced the Bill in May 2011, which has the same goals as COICA, including cracking down on the websites who supply the infringing content.[6] This in turn makes it tougher for consumers to access pirated films and shows on the web. Thus, the most effective way to evaluate the Protect IP Act is to examine COICA, also called Senate Bill 3804, because many of the same assets and challenges posed to Senate Bill 3804 are relevant to the present discussion regarding the Protect IP Act.

This paper will focus exclusively on an analysis of Senate Bill 3804, which gives the Justice Department the ability to bring an in rem action against a domestic domain name used by an Internet site that is "dedicated to infringing activities."[7] After the Attorney General obtains a court order, the Justice Department can serve the court order on the "domain name registrar or, if the domain name registrar is not located within the United States, upon the registry"[8] in order to stop that domain name from resolving into the infringing website's IP address. For example, if a court order was obtained against a website, when a user enters that website's URL address into their web browser, the person would not be able to reach that website. This would be effective because one generally does not memorize an IP address, but rather one memorizes a domain name. Furthermore, a search engine result is listed as a domain name, not an IP address. Therefore, unless the user knows what the IP address is for a particular website with infringing material, if the domain name is removed from the registry, he or she will not be able to reach that website.

The Bill also gives the Department of Justice the power to shut down international websites that feature pirated material by cutting off their sources of support (the supply side), such as internet service providers (ISPs), financial transaction providers such as PayPal, and advertisers. This likely is the most effective approach because it targets the core sources that indirectly facilitate the infringers in completing their task. By eliminating an advertiser through the supply side approach, instead of a user in a demand side approach, the Justice Department could more effectively combat and shut down websites

[5] Larry Downes,*Leahy's Protect IP bill even worse than COICA*, CNET, http://news.cnet.com/8301-13578_3-20062419-38.html May 12, 2011.

[6] S. 968, *Protect IP Act of 2011*, http://www.opencongress.org/bill/112-s968/show .

[7] Combating Online Infringement and Counterfeits Act ("COICA"), S. 3804, 111th Cong. §2(a)(1) (2010).

[8] S. 3804, 111th Cong. § 2(e)(1) (2010).

dedicated to intellectual property piracy. Instead, going after individual users would, aside from being very inefficient, certainly have much less of an impact on the infringing website.

The Recording Industry Association of America (RIAA) has made attempts to enforce copyrights on the demand-side, but litigation was very expensive and a public relations nightmare for record companies. For example, in *Sony BMG Music Entertainment v. Tenenbaum*,[9] several record companies sued a college student, Joel Tenenbaum, for copyright violations, accusing him of illegally downloading and sharing thirty copyright protected songs.[10] The jury decided against Tenenbaum and awarded the record companies $675,000.[11] In July 2010, United States District Court Judge Nancy Gertner reduced the judgment to $67,500.[12] Moreover, Tenenbaum was able to paint himself more as a David versus Goliath, saying that the record company lawyers were "bankrolled by multibillion-dollar corporations, throwing everything they had at someone who wanted to share Come As You Are with other Nirvana fans."[13] Suing on the demand side was also very ineffective since there are so many people who access infringing content, leading to a "whack a mole approach" because it is too difficult to target the "demand-side."[14]

This paper will assert that exercising jurisdiction over domestic and foreign websites is a strong attribute of the Bill given both the current state of pirated websites originating from international locations and the lack of supply-side legislation in other countries. The main thrust of Senate Bill 3804 is that it would grant the Attorney General the power to seek a court injunction against a domain name to halt illegal activities.[15] The Bill goes after intermediaries precisely when

---

[9] 672 F. Supp. 2d 217(D. Mass. 2009).

[10] *Id.* at 219.

[11] Matthew Friedman, comment, *Nine Years and Still Waiting: While Congress Continues to Hold Off on Amending Copyright Law for the Digital Age, Commercial Industry Has Largely Moved on*, 17 VILL. SPORTS & ENT. L.J. 637, 654-55 (2010).

[12] Rodrique Ngowi, *Judge Cuts Penalty in Song-Sharing Case*, THE ASSOCIATED PRESS (July 10, 2010), http://www.usatoday.com/tech/news/2010-07-09-song-sharing-penalty-cut_N.htm.

[13] Joel Tenenbaum, *How It Feels to Be Sued for $4.5m*, THE GUARDIAN (July 27, 2009), http://www.guardian.co.uk/music/musicblog/2009/jul/27/filesharing-music-industry.

[14] Cecillia Kang, *Facebook, Google join to fight Internet piracy legislation*, THE WASHINGTON POST, (Nov. 15, 2011).

[15] S. 3804, 111th Cong. 2(b).

jurisdiction cannot be exercised over the websites.[16] When it can be, the Bill calls for seizure of the domain name.[17] Since this landmark legislation has an opportunity to lead to progress in curbing infringing web-based material, it is important to consider the best arguments on both sides of the discussion. Therefore, the purpose of the paper is to analyze the constitutionality of the amended Senate Bill 3804, COICA, and to evaluate the Bill's pros and cons. The paper will analyze the arguments for and against the Bill by drawing upon case law that helps to inform the discussion of balancing the values served by constitutional protections such as freedom of speech and protection of the rights of copyright holders.

II. EXPLANATION OF THE BILL

What constitutes an infringing website? COICA defines a website to be dedicated to infringing activities if it is "primarily designed, or has no demonstrable commercially significant purpose or use other than. . .offering or providing access in a manner not authorized by the copyright ownerFalse"[18] The Bill's definition includes websites that offer infringing movies for download, streaming, or provide a link to these options.[19] For example, a website that offers pirated movies for users to download could face a temporary restraining order.

A. DOMESTIC WEBSITES

If a domestic website contains allegedly infringing content, under the Bill's provisions, there are several steps that the Justice Department takes. In order to begin action in federal court, the Attorney General must first send a notice of an alleged violation to the domain name registrant.[20] Next, the Attorney General publishes a notice of the action according to the court's instructions, and sues the domain name registrant.[21] The Attorney General then serves the court order on the domain name registry and the domain name registrar, which will have to "suspend" activities and "may lock" the domain name.[22] Once the

16 *Id.* at 2(e)(2)(A).
17 *Id.* at 2(e)(1).
18 S. 3804, 111th Cong. § 2(a)(1)(B)(i)-(I) (2010).
19 *Id.*
20 *Id.* § 2(c)(1)(B)(i).
21 *Id.* § 2(c)(1)(B)(i).
22 *Id.* § 2(e)(1).

Attorney General initiates an in rem action against the alleged infringing domain name, the court can issue an injunction against that domain name to demand that the website "cease and desist" the infringing activity.[23] Thus, the domain name registrant is given notice early on in the proceedings so that it is aware of the alleged infringing activity, and has an opportunity to stop such illegal actions early.

For domestic websites, there is something akin to a "bad actor list." Once the Attorney General notifies the Intellectual Property Enforcement Coordinator of a court order against a domain name, the Coordinator is required to post the domain name on an internet site.[24] The Bill provides that this website would be accessible to the public.[25] Thus, it would alert the actual and virtual community to any website with infringing content.[26] This puts the public on notice that it is downloading or streaming infringing content, but it is also a form of public shaming. Moreover, it may deter other websites from popping up if potential creators see that the other websites with infringing content have been detected and are facing or have faced consequences.

B. NONDOMESTIC WEBSITES

One noteworthy aspect of Senate Bill 3804 is that it enables the Justice Department to target internationally registered websites. Similar to the process with domestic websites, in order to begin the action in federal court, the Attorney General first sends a notice of an alleged violation to the domain name registrant.[27] Next, the Attorney General publishes a notice of the action according to the court's instructions, and sues the domain name registrant.[28] The proposed statute states that if a court order is received and the domain is registered outside the United States, the Attorney General may, but likely will serve the court order on intermediaries, including service providers,[29] financial transaction providers,[30] and advertisers.[31] Given that the Justice Department would be able to take these comprehensive steps for a website originating from

---

[23] *Id.* § 2(b).
[24] S. 3804 § 2(f).
[25] *Id.*, § 2(f).
[26] *Id.*
[27] *Id.* § 2(c)(1)(B)(i)
[28] *Id.* § 2(c)(1)(B)(i)-(ii).
[29] *Id.* § 2(e)(2)(B)(i).
[30] S. 3804, § 2(e)(2)(B)(ii).
[31] *Id.*, § 2(e)(2)(B)(iii).

a source outside our nation's borders, the Bill goes to great lengths to determine if it indeed targets United States consumers in the first place. Factors that the court considers in this analysis include whether there is evidence that the website is intended to provide an illicit service or good or access to these goods or services to a U.S. consumer,[32] whether the website has "reasonable measures"[33] to prevent these goods or services from being accessed in the United States, and whether the prices for the goods are in U.S. currency.[34] These indicia help guarantee that there are certain jurisdictional prerequisites and criteria that the Justice Department would have to use in order to justify its decision to go after an internationally based website. Given these specifications, these criteria are also an effective response to critics who decry the Bill as granting the U. S. government too much leeway in making determinations over which websites to target.

If the domain is registered outside the United States, there are numerous implications for the website.[35] The definition of an infringing website also has an internationally-minded framework built into its terms.[36] The definition's use of the phrase "providing access" encompasses peer-to-peer indicies such as the Pirate Bay, a notorious conduit for infringement described as a website "that provide[s] links to copyrighted works, even if the actual BitTorrent streams are hosted elsewhere."[37] To proceed against a website, the Attorney General files a lawsuit (an in rem action) against the website's domain name in the District of Columbia.[38] If a court order is received and the domain is registered outside of the United States, the Attorney General can act against the domain by serving the court order on three types of companies which enable the website to be accessible within the United States: internet service providers, financial transaction providers, and advertisers.[39]

---

[32] *Id.* § 2(d)(2)(B)(i)-(ii).

[33] *Id.* § 2(d)(2)(B)(iii).

[34] *Id.* § 2(d)(2)(B)(iv).

[35] *Id.* at 2(e)(2)(B).

[36] S. 3804, 2(d)(2)(B).

[37] Declan McCullagh, *Piracy Domain Seizure Bill Gains Support*, CNET (Nov. 9, 2011, 8:00 PM), http://news.cnet.com/8301-13578_3-20020408-38.html#ixzz144lLZzNy.

[38] S. 3804, § 2(d)(2)(A).

[39] *Id.* § 2(e)(2)(A)-(B).

i. Internet Service Providers

The targeting of internet service providers does not apply to domestically registered websites, but only internationally registered websites.[40] An internet service provider must, "as expeditiously as reasonable[,] take technically feasible and reasonable steps" to prevent the website name from finding its IP address.[41] In practice, the Attorney General would obtain an injunction preventing domain name servers in the United States from translating the website's URL into a numeric IP address.[42] In other words, the domain name servers would prevent computers from being able to reach that website. However, the ISP does not have to "change its network to comply with the order."[43] Moreover, the ISP does not have to take any measures "with respect to domain name lookups not performed by its own domain name system server. . ."[44] Basically, this means that the ISP does not have to police other servers.

ii. Financial Transaction Providers

The targeting of financial transaction providers does not apply to domestically registered websites. For internationally registered websites that infringe upon copyrighted material, a "financial transaction provider" must take "reasonable measures, as expeditiously as reasonable"[45] to prevent financial transactions between the U.S. customers and the website that has infringing material. This means that if a website allows a user to download a pirated film for two dollars and uses a "financial transaction provider" such as Paypal to process the transaction, the Attorney General may serve the court order to Paypal ordering it not to process the transaction.[46] Paypal would be required to stop processing U.S. customers' transactions for that domain name and to stop allowing its trademark to be used on the website with the infringing content.

---

40 *Id.* §2(e)(2)(B)(i).
41 *Id.* § 2(e)(2)(B)(i).
42 *Id*. §2(e)(2)(B)(i).
43 *Id.* § 2(e)(2)(B)(i)(I)(aa).
44 S. 3804 § 2 (e)(2)(B)(i)(I)(bb).
45 *Id.* § 2(e)(2)(B)(ii).
46 S. 3804, 111th Cong..§ 2(e)(2)(B)(ii)(I) (2010).

iii. Advertisers

The targeting of advertisers also does not apply to domestically registered websites. The Attorney General may serve the court order to an advertising service ordering it to take "reasonable measures, as expeditiously as reasonable" to cease advertising on the website.[47] This is an incredibly important provision because at the heart of many of these websites is that they may offer the film for free in order to attract users to the website. After all, part of the allure of a movie website to the consumer is obtaining the infringing content for free. Thus, these websites earn money by demonstrating to advertisers that the website is accessed by a large amount of people.

Moreover, as demonstrated by the *Grokster* case below, showing that the company does not directly financially profit from the infringement,since users do not pay for the content, could sometimes help the company in escaping liability.[48] On the other hand, *Grokster* also decided that one infringes vicariously by profiting from direct infringement by not exercising a right to stop it.[49] This provision in the Bill solidifies part of the Court's holding in *Grokster*. In that case, even though Grokster did not charge users for accessing the infringing content, the company did reap a financial reward from advertisers doing business with the website.[50] If the advertisers were unable to exist, it would be unlikely that a company such as Grokster would have an incentive to still provide its service.[51]

III. AREAS WHERE THE BILL COULD BE STRENGTHENED

Even though the proposed Bill would give greater power to the Justice Department to target the supply side of the website through its internet service provider, advertisers, and financial transaction providers doing business with the website, the terms "reasonable measures, as expeditiously as reasonable" are relatively vague and may necessitate further specifications.[52] Any of the above three entities (domain name registry, financial transaction provider and advertiser) who take action in order to comply with the court order will be immune from any federal

[47] *Id.* § 2(e)(2)(B)(iii).
[48] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 914 (2005).
[49] *Id.*
[50] *Id.* at 913.
[51] *Id.*
[52] S. 3804, 111th Cong. § 2(e)(2)(B)(ii)(I) (2010).

or state action against any act reasonably taken to comply with the order.[53] Just as with domestic websites, there is also a "bad actor" list with regard to international websites. Once the Attorney General notifies the Intellectual Property Enforcement Coordinator (the Coordinator is responsible for "implementing the Administration's overall [intellectual property enforcement] strategy"[54]) of a court order against a domain name, the Coordinator is required to post the domain name on a "publically available internet site."[55] The bad actor list's website would be accessible to the public and thus would alert consumers to any website with the infringing content.[56]

But would the Bill be realistically enforceable? A concern might be that an entity that creates an infringing website may be able to easily change the website name very slightly once it is caught. However, Senate Bill 3804 addresses this issue. According to the Bill, the Attorney General may apply to have a court order modified to include similar or reconstituted domain names.[57] There is an opportunity, however, to make a change or undo the order, which actually can function as an incentive for a website to stop posting illegal content. The website owner or registry owner can petition the court to modify or revoke the order if the domain name registry expires, or, for example, once a domain name stops posting pirated movies.[58]

IV. ARGUMENTS AGAINST SENATE BILL 3804

The opponents to Senate Bill 3804 include the Center for Democracy & Technology (CDT), the Electronic Frontier Foundation, and the Distributed Computing Industry Association.[59] In response to criticism,[60] Senator Patrick Leahy (D-VT), one of the Bill's sponsors,

---

[53] *Id.* § 2(e)(5)(A).

[54] Office of the U.S. Intellectual Property Enforcement Coordinator, THE WHITE HOUSE, http://www.whitehouse.gov/omb/intellectualproperty/bio_espinel (last visited Oct. 12, 2012).

[55] S. 3804, § 2(f).

[56] *Id.*

[57] *Id.* § 2(h)(1)(A).

[58] *Id.* § 2(h)(2).

[59] *S. 3804 Combating Online Infringement and Counterfeits Act*, GOVTRAK.US, http://www.opencongress.org/bill/111-s3804/show (last visited Nov. 9, 2011).

[60] Jaikumar Vijayan, *Outcry prompts amendments to online IP protection bill*, ComputerWorld, http://www.computerworld.com/s/article/9188780/Outcry_prompts_amendments_to_online_IP_protection_bill, (Sept. 29, 2010).

amended the Bill with other legislators on September 29, 2010 as a result of criticism from digital rights groups such as the Electronic Frontier Foundation and high-tech engineers.[61] Thus, it may have neutralized some of the opposition's concerns. The Bill that the Senate Judiciary approved on November 18, 2010, has incorporated the September 29, 2010 amendments in their entirety. Thus, the paper will compare the original proposed version to its most current form. The November 18, 2010 Bill contains four major revisions.

First, the original Bill contained a separate provision for action on the part of the Attorney General without the necessity for a court order.[62] The Attorney General was authorized to post websites that are suspected of being primarily dedicated to infringing activity on a publicly accessible list.[63] Companies, such as internet service providers, would be allowed to voluntarily take actions to prevent public access to those websites and would be immune from any legal action as a result.[64] In other words, the Attorney General, by listing the suspected infringing website on a list without having to seek a court order and allowing a company to take action accordingly, would have free reign to use its office to limit access to suspected infringing websites without the judicial system's approval.[65] The only check on this power was that a website would retain the right to petition a court to be removed from this list.[66] These two provisions were stricken completely from the amended Bill.

Second, the original Bill directed internet service providers served with a court order against a website to "take reasonable measures" to prevent users from accessing infringing websites, and it directed financial transaction providers served with the same court order to "take reasonable measures" to block transactions for that website.[67] However, there was no explanation as to how to define "reasonable" or how far these providers were required to go to comply with the court order. The amended Bill now guides internet service providers to "take technically

---

[61] Cecilia Kang, *Senate Piracy Bill Changed After Criticism by ISPs, Engineers, Public Advocates*, WASH. POST., Sept. 29, 2010, http://voices.washingtonpost.com/posttech/2010/09/senate_piracy_bill_changed_aft.html.

[62] S. 3804, §2(j)(1). (as introduced by Senate, Sept. 20, 2010).

[63] S. 3804, § 2 (2324)(j)(1-2) (as introduced by Senate, Sept. 20, 2010).

[64] *Id.* § 2 (2324)(j)(2) (as introduced by Senate, Sept. 20, 2010).

[65] *Id.* § 2 (2324)(j)(1)-(2) (as introduced by Senate, Sept. 20, 2010).

[66] *Id.* § 2 (2324)(j)(4)(A) (as introduced by Senate, Sept. 20, 2010).

[67] *Id.* § 2 (2324)(e)(2)(B)(i) (as introduced by Senate, Sept. 20, 2010).

feasible and reasonable steps" to comply with the court order.[68] Specifically, an internet service provider would not be required to "modify its network of other facilities[,]" "take any steps. . .not performed by its own domain name server[,]"or "prevent access" to a website when it "has been effectively disabled by other means."[69] The amended Bill directs financial transaction providers to act "as expeditiously as reasonable," but no more specific elaboration has been added.[70]

Third, the original Bill provides immunity from "action . . . in any Federal or State court or administrative agency."[71] The amended Bill contains the same language, but also more explicitly states that those acting to comply with a court order "shall not be liable to any party for any acts reasonably designed to complyFalse"[72] Fourth, not present in the original Bill, the amended Bill legislates cooperation with other enforcement agencies by requiring that the Attorney General "develop a deconfliction process in consultation with other law enforcement agencies. . .to coordinate enforcement activities. . . ."[73]

A. First Amendment

The CDT stated that Senate Bill 3804 violates the First Amendment because it could require a court to impose a prior restraint on speech.[74] The organization states that Senate Bill 3804 would overstep the bounds of *Nebraska Press Association v. Stuart*,[75] because even if it blocked illegal content, in doing so, it would also restrict lawful material. In fact, a *Los Angeles Times* editorial may have referred to CDT when it argued that "[s]ome technology advocates and public interest groups also have warned that the [B]ill's domain-name

[68] *Id.* § 2(e)(2)(B)(i).

[69] S. 3804, § 2(e)(2)(B)(i)(I)(aa)-(cc).

[70] *Id.* § 2(e)(2)(B)(ii)(I).

[71] *Id.* § 2 (2324)(e)(3) (as introduced by Senate, Sept. 20, 2010).

[72] S. 3804, 111th Cong. § 2(e)(5)(A) (2010).

[73] *Id.* § 3(6).

[74] *The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*, CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/report/dangers-s3804-domain-name-seizures-and-blocking-pose-threats-free-expression-global-internet- (last visited Oct. 12, 2011).

[75] *The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*. CENTER FOR DEMOCRACY AND TECHNOLOGY, (Sept. 28, 2010).

provisions would violate free-speech principles — because some legitimate content may exist alongside pirated material on blocked sites."[76] In *Stuart*, the Supreme Court invalidated a trial judge's order that was designed to prevent reporters from disseminating incriminating information about a criminal defendant.[77] The Supreme Court relied in part on the rules against prior restraints to invalidate the order.[78] The Court noted that the restraining order would be difficult to police.[79] The CDT says the Bill would violate the First Amendment because it is not "narrowly tailored" to meet constitutional requirements such as those announced in *Stuart*.[80] However, CDT fails to acknowledge that preliminary injunctions are granted in copyright infringement cases "as a matter of course."[81] In his article, Eugene Volokh explains that the Supreme Court, in *Harper & Row, Publishers, Inc. v. Nation Enterprises*,[82] held that the First Amendment does not protect copyright infringing speech.[83] To avoid chilling free speech, facts and ideas are not copyrightable, and there also is a fair use exception.[84] "Copyright, the Court said, is itself an 'engine of free expression' because it 'supplies the economic incentive to create and disseminate ideas.'"[85]

Senate Bill 3804 suppresses only the websites whose primary purpose has been found to engage in the distribution of pirated films, which is already an illegal act. In fact, the very definition used in COICA is that the website would have to be "primarily designed" or have "no demonstrable commercially significant purpose" other than

---

[76] Editorial, *Sinking the online pirates*, LOS ANGELES TIMES, November 28, 2010, http://www.latimes.com/news/opinion/editorials/la-ed-piracy-20101128,0,7950612.story

[77] *The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*. CENTER FOR DEMOCRACY AND TECHNOLOGY, (Sept. 28, 2010).

[78] *Id.*

[79] Nebraska Press Association v. Stuart, 427 U.S. 539, 565-66 (1976) ("The need for *in personam* jurisdiction also presents an obstacle to a restraining order that applies to publication at large a distinguished from restraining publication within a given Jurisdiction.").

[80] *The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*. CENTER FOR DEMOCRACY AND TECHNOLOGY, (Sept. 28, 2010).

[81] Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 150 (1998).

[82] 471 U.S. 539 (1985).

[83] Lemley & Volokh, *supra* note 81, at 166.

[84] *Id.* at 194.

[85] *Id.* at 166.

infringement.[86] The provision means that not only would it be clear that the website's goal was to violate copyright law, but also that there would be nothing of value left in the website that would be stifled if others were prevented from accessing it.

B. Fifth Amendment

The Bill also comports with the Fifth Amendment. In addition to the Fifth Amendment limiting law enforcement in its use of illegally obtained evidence, it also includes the privilege against self-incrimination: "nor shall be compelled in any criminal case to be a witness against himself."[87] Law enforcement can basically compel ISPs to release information: "the entire internet world of stored internet communications can be subpoenaed via the intermediaries of ISPs."[88] The only standard is that the information be relevant to the investigation, which is a relatively low threshold.[89] The "Fifth Amendment [defense] fails because third parties such as ISPs can divulge information without implicating any privilege against self-incrimination of their own."[90] This means that a third party cannot invoke the Fifth Amendment. In other words, the ISP itself is innocent; it has not done anything wrong, so it cannot assert the Fifth Amendment privilege of self-incrimination because there is no information from the subpoena that can implicate them in anything. The information can implicate the person creating a website that features a pirated movie.

Additionally, the CDT argues that the ability for the Attorney General to seek a preliminary injunction functions as a prior restraint and, in the case of Senate Bill 3804, does not meet the requisite procedural safeguards.[91] These include a full hearing on the case's merits with parties in attendance.[92] Critics have stated that the Bill denies due process to website operators "due to the unreasonable demand of having to travel from around the globe in order to appear in a

[86] S. 3804, 111th Cong. § 2 (a)(1)(B)(i)-(I) (2010).

[87] U.S. CONST. amend V.

[88] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 296 (2005).

[89] *Id.* at 297.

[90] *Id.* at 296.

[91] *The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture*. CENTER FOR DEMOCRACY AND TECHNOLOGY, (Sept. 28, 2010).

[92] *Id.*

U.S. courtroom to fight the claims of copyright infringement."[93] The response to this concern is that if a web operator sponsors a website with alleged pirated movies, and thus is allegedly engaging in illegal behavior that affects the United States, they should be prepared to travel to the United States to defend their claim or hire a U.S. lawyer. The Bill indeed considers several factors to determine if the website targets a U.S. audience. These include the following: (1) whether the website provides infringing material to a U.S. user;[94] (2) whether there is evidence that the website is not intending to provide the goods, their access or the delivery of the infringing material to a U.S. user;[95] (3) whether there is evidence that the internet site has "reasonable measures to prevent" the infringing material to be acquired in the United States;[96] (4) whether the website offers services acquired in the United States;[97] and (5) whether the price for the infringing material is listed in U.S. dollars.[98] Once the court considers these factors, it would be able to determine "whether an Internet site conducts business directed to residents of the United States."[99] If that is the case, there certainly is a strong argument that that the website operators would have the resources and incentives to protect their interests in a hearing.

C. Fourth Amendment

An additional concern involves the Fourth Amendment. The Fourth Amendment guards against unreasonable searches and seizures.[100] The Fourteenth Amendment applies the Fourth Amendment to the states.[101] In *Rehberg v. Paulk*[102], and *United States v. Ahrndt*[103], federal courts looked at whether the government violates the Fourth

---

[93] Jared Moya, *U.S. Chamber of Commerce: "Censoring Foreign P2P sites Not Censorship,"* ZEROPAID (Sept. 29, 2010), http://www.zeropaid.com/news/90904/us-chamber-of-commerce-censorin-foreign-p2p-sites-not-censorship/

[94] S. 3804, 111th Cong. § 2(d)(2)(B)(i) (2010).

[95] *Id.* § 2(d)(2)(B)(ii).

[96] *Id.* § 2(d)(2)(B)(iii).

[97] *Id.* § 2(d)(2)(B)(iv).

[98] *Id.* § 2(d)(2)(B)(v).

[99] *Id.* § 2(d)(2)(B).

[100] U.S. CONST. amend. IV.

[101] *See* U.S. CONST. amend. XIV.

[102] Rehberg v. Paulk, 611 F.3d 828, 835 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678, (U.S. 2011).

[103] United States v. Ahrndt, No. 08-468, 2010 WL 373994, at *5-7 (D. Or. Jan. 28, 2010).

Amendment when it accesses evidence of illegal conduct on the web. The interesting aspect of cybercrime is that, without even realizing it, a user stores "most if not all of their private information on remote servers."[104] In certain situations, a police officer may no longer have to enter someone's home and look into the physical contents of their computer. The digital world is no longer necessarily anchored in physical objects.

In *Rehberg v. Paulk*, the Eleventh Circuit held that a person does not have a reasonable expectation of privacy in an email once he sends it and it is stored at an ISP.[105] In the case, Charles Rehberg anonymously sent faxes to a hospital criticizing its management.[106] To find out more information, the Chief Investigator in the District Attorney's Office James Paulk subpoenaed the Internet service provider Rehberg used for his email.[107] Paulk then accessed '"Rehberg's personal e-mails that were sent and received from his personal computer."[108] Rehberg sued Paulk claiming that the investigation violated his Fourth Amendment right against unreasonable search.[109]

For the Fourth Amendment to come into play, a person must have an objectively reasonable expectation of privacy in the place searched or the item seized."[110] To meet the threshold of a reasonable expectation of privacy, one must show two elements: "(1) that he manifested 'a subjective expectation of privacy' in the item searched or seized, and (2) a willingness by society 'to recognize that expectation as legitimate."[111] Among the cases the court used to support its holding, the court cited the Sixth Circuit case *Guest v. Leis*,[112] which held that there is no Fourth Amendment expectation of privacy in a bulletin board on the web.[113] Much like an internet bulletin board message, using the analysis from *Rehberg*, a person who posts a pirated movie and its associated contents online should certainly not rely on a Fourth Amendment expectation of

---

104 Kerr, *supra* note 86, at 293.

105 *Rehberg*, 611 F.3d at 847.

106 *Id.* at 835.

107 *Id.*

108 *Id.*

109 *Id.* at 836-37.

110 *Id.* at 842.

111 Rehberg v. Paulk, 611 F.3d 828, 843-44 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678, (U.S. 2011).

112 255 F.3d 325, 333 (6th Cir. 2011).

113 *Id.*; *see also Rehberg*, 611 F.3d at 843-44.

privacy.

Federal courts have also held that there was no reasonable expectation of privacy when someone posts a file to be shared with another internet user such as one who uses iTunes to share files on an unsecured wireless connection.[114] In *United States v. Ahrndt*, a woman the court referred to as "JH" used her personal computer at home to connect to her wireless network.[115] When the wireless network stopped working, her computer instantaneously connected her to her neighbor's unsecured network.[116] Since the connection transfer was automatic, JH did not know she was no longer on her network.[117] Since JH and her neighbor were on the same wireless network and had their iTunes on a "shared" setting, when JH opened her iTunes program, she was able to look into another person's music and video library. When JH looked into the neighbor's files, she saw titles that referred to child pornography.[118] JH contacted law enforcement.[119] As a result, the Department of Homeland Security obtained two search warrants: one to determine the IP address that accessed the wireless network and another to search the home of whoever owned the IP address.[120] The name behind the IP address turned out to be John Henry Ahrndt, a convicted sex offender.[121]

Ahrndt filed a motion to suppress the evidence seized based on a Fourth Amendment violation.[122] The court ruled against Ahrndt, explaining that there is a long judicial history of distinguishing a person's reasonable expectation of privacy depending on the situation.[123] For example, a person has a different reasonable expectation of privacy depending on whether the technological device is a wireless network secured by a password as opposed to one without. A person is more likely to inadvertently intercept another user's files, so that when one logs onto a wireless network, he has implicitly accepted that reduced

---

[114] United States v. Ahrndt, No. 08-468, 2010 WL 373994, at *5-7 (D. Or. Jan. 28, 2010).

[115] *Id.* at *1.

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id*.

[120] *Ahrndt*, 2010 WL 373994 at *1-2.

[121] *Id.* at *1.

[122] *Id.* at *2.

[123] *Id.* at *3.

expectation of privacy.[124] Ahrndt took no steps to keep the data on his computer secure when he used the iTunes "sharing" function and did not secure his network with a password. Also, iTunes' default setting does not automatically share files.[125] Ahrndt's library of illegal materials was set up to be shared. Thus, the court held that using a computer that voluntarily shares files on iTunes through an unsecured connection is "like leaving one's documents in a box marked 'take a look' at the end of a cul-de-sac."[126] Much like iTunes' "shared" function, pirated films on websites are intended to be accessed by others. These films are featured on an open network not only granting permission for others to view like in the *Ahrndt* case, but going even further since these websites encourage third party access by offering the movies for free. The website operator has a diminished expectation of privacy because the website is designed to be open for global access, and thus certainly cannot be considered to be private.

As a final point, the CDT argues that IP addresses can easily be disguised, thus circumventing the restrictions. Circumvention technology will always exist, and if anything, that means that the Bill's provisions might be broader, allowing the legislation to evolve to account for cracking down on the circumvention technology. For example, the Bill could require a website to disclose whether it is using circumvention technology and if so, describe the person(s) from whom search technology was purchased or obtained. The failure to enact Senate Bill 3804 into law will not lessen the fact the IP addresses will be disguised. The Senate Bill may even incentivize further technology that will assist in detecting a disguised IP address because there will be a need for such innovation.

Moreover, despite the fact that a subpoena would uncover evidence that would potentially incriminate the alleged infringer, law enforcement does not even need to notify the alleged infringer because they are not being subpoenaed, a third party would be. "The person under investigation need not be informed of the subpoena's existence."[127] Although usually we think of the subpoena power as generally very restricted, when dealing with "computer crime. . .it is incredibly broad. For investigators, compelling the ISP to disclose

[124] *Id.* at 4.
[125] *Id.* at *7.
[126] *Ahrndt*, 2010 WL 373994 at *7.
[127] Kerr, *supra* note 86, at 294.

information is even preferable to the alternative of searching through the ISP's server directly: Officers can simply fax a copy of the subpoena to the ISP's headquarters and await a package or return fax with the relevant documents."[128] Thus, the constitutional language of a "search" is no longer directly implicated.

D. Additional "Attacks" on the Bill

An additional attack on the Bill is that "notice and take down" provisions already exist as law. In *Viacom v. YouTube*, the District Court held that although users are constantly uploading copyrighted material to YouTube, the website publisher can take shelter in the Digital Millennium Copyright Act. [129] The DMCA protects a website such as YouTube if it follows the DMCA's "notice and take-down" rules, meaning that as soon as the website has notice of infringing content on the website, it must take the content down.[130] Viacom sued the video sharing website claiming that YouTube participated in copyright infringement by allowing users to post their copyrighted videos without the company's permission.[131] The court stated that while YouTube was generally aware that users were engaging in copyright infringement, it would be unreasonable to hold YouTube accountable since it was unaware which specific clips were uploaded without permission.[132] The issue is whether to put the burden on the website or the content holder. Courts in cases such as *YouTube* and *Io Group, Inc. v. Veoh Networks, Inc*.[133] place the burden on the content holder.[134] If the *YouTube* case were to be reversed on appeal, however, the burden would be on the website to police the content on its website for copyright violations. In its safe harbor provisions, the DMCA deals with the registrant, also known as the website, such as YouTube.[135] In contrast, Senate Bill 3804 shuts down a domestic website through the

---

[128] *Id,* at 296.

[129] *See* Viacom Intern., Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 526 (S.D.N.Y. 2010).

[130] Eriq Gardner, *Viacom vs. YouTube unsealed! YouTube's Steve Chen on copyrighted content: 'Steal it!'* (Dec. 21, 2010), http://www.hollywoodreporter.com/blogs/thr-esq/viacom-youtube-unsealed-youtubes-steve-63731.

[131] *YouTube*, 718 F. Supp. 2d at 516.

[132] *Id.* at 523.

[133] 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

[134] *Id.* at 1141.

[135] 17 USCA § 512 (c)(1)(A)(iii).

domain name registrar, such as godaddy.com.[136] Thus, Senate Bill 3804 is still necessary in the fight against infringing material on the internet.

A *Los Angeles Times* editorial further criticized the Bill by stating that when a court orders "the registrar or registry to invalidate the [infringing] website's domain name" it is "akin to ordering road atlases to erase a street from their maps — it would still be there, but it would be much harder to find."[137] The editorial argues that a user could still potentially type in the IP address and reach the infringing website despite the fact that the domain name is removed from the registry. From a practical standpoint, however, people do not navigate to a website by typing in the IP address in the browser. Rather, a user searching for an infringing website would type the domain name in the browser or search for that domain name through a search engine. Thus, the Bill is not merely asking the atlas to erase a street name; it is also changing the landscape.

V. ARGUMENTS FOR THE BILL

The Bill has garnered support throughout the entertainment industry. Proponents of the Bill include the Motion Picture Association of America (MPAA), the Directors Guild of America (DGA), the Screen Actors Guild (SAG), the Writers Guild of America West (WGAW),[138] Viacom, the United States Chamber of Commerce, the International Alliance of Theatrical Stage Employees (IATSE), and the Allied Crafts of the United States.[139] These organizations contend that the Bill is necessary to protect the movie industry's business. Given that pirated films are becoming more abundant on the internet, the Bill would be an effective way to combat piracy at its source.

Court precedent provides additional support for the Bill. The Supreme Court held in *MGM Studios, Inc. v. Grokster, Ltd*. that "one who distributes a device[, such as file-sharing software,] with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement is liable for the

---

[136] S. 3804, 111th Cong. §2(e)(1) (2010).

[137] Editorial, *Sinking the online pirates*, LOS ANGELES TIMES, (Nov. 28, 2010), http://www.latimes.com/news/opinion/editorials/la-ed-piracy-20101128,0,7950612.story.

[138] Press Release, Writers Guild of America, Writers Applaud Anti-Piracy Bill (Sept. 29, 2010), *available a*t http://www.wga.org/content/default.aspx?id=4346.

[139] *S. 3804: Combating Online Infringement and Counterfeits Act*, http://www.opencongress.org/bill/111-s3804/show (last visited Nov. 9, 2011).

resulting acts of infringement by third parties[,]" even where the device has substantial non-infringing uses.[140] The Court found evidence of inducement in three ways: (1) Grokster targeted the "market. . .of former Napster users" by supplying the peer to peer network service to them; (2) Grokster did not try to develop a filtering tool to reduce the likelihood of infringing activity; and (3) Grokster made money by selling ads, the ads were more profitable as more users used the service, and the evidence showed that users used the service for infringement.[141] Much like in *Grokster*, the websites that would be shut down under the Bill would be "good for nothing else" but infringement.[142] If a website features an infringing movie for a free download, the website, like Grokster, may profit by selling ad space. The Supreme Court noted in *Grokster* that a peer to peer network that induces infringement can be held accountable.[143] Senate Bill 3804 codifies that accountability by providing the Justice Department with the capacity to get a court order to suspend the operation of the domain name of a domestic website and target the sources of support for an international website that induces infringement.[144]

VII. CONCLUSIONS ON WHY THE BILL IS OR IS NOT CONSTITUTIONAL

On the one hand, one could make the argument that the Bill is likely too broad (Viacom refers to it as having "flexibility"[145]) to pass constitutional muster because it is not sufficiently "narrowly tailored." For example, CNET writer Greg Sandoval stated: "they haven't given us a criterion of how they're going to decide a website is a pirate website. And a judge either has to be really informed, really skeptical to challenge these guys."[146] However, according to Senator Orrin Hatch (R-Utah), as he stated in the Congressional Record, the Bill has built in "safeguards" to prevent the Justice Department from abusing its powers:

---

[140] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 925-27 (2005).

[141] *Id.*

[142] *Id.*

[143] *Id.* at 941.

[144] S. 3804, 111th Cong. §(2)(e) (2010).

[145] Viacom Inter., *Viacom Supports Senate's Infringement Bill*, GAMEPOLITICS.COM, Sept. 21, 2010, http://gamepolitics.com/2010/09/21/viacom-supports-senate%E2%80%99s-infringement-bill.

[146] Transcript from "On the Media," http://www.onthemedia.org/transcripts/2010/09/24/04.

"For example, a Federal court would have the final say as to whether a particular website would be cut off from supportive services. In addition, the Bill would allow owners or website operators to petition the court to lift the order."[147] While some critics may argue that the Justice Department's ability to petition a court to shut down a website based on its (albeit illegal) content gets close to the zone of censorship, the proposed statute states that the website owner, for example, can petition to get rid of the order if the "interests of justice require" such action.[148] This open-ended standard could potentially allow those who would have compelling arguments to state their case. Although *Rehberg v. Paulk* was decided in July 2010, the Eleventh Circuit Court of Appeals noted that "only a few circuit decisions address the issue of Fourth Amendment protection of email content."[149] At this point, I think the Bill has an effective means of targeting websites whose principal business is to purvey infringing content. Thus, the Bill need not be improved to help eradicate piracy "at the source" in a constitutional manner.

VII. "COMING ATTRACTIONS": COMPARABLE INTERNATIONAL LEGISLATION?

There really is no comparable legislation or practices developing elsewhere in the world that can be looked at for instruction or to follow its example. It seems that international legislation, at this point, does not offer a way to improve the Bill. The reason behind writing about it briefly below is because one of the justifications for the Bill's targeting of foreign websites, according to the U.S. Chamber of Commerce, is because it's needed since foreign legislation does a poor job.[150] Perhaps the foreign legislation would do a better job if it was "supply-side" focused. New Zealand and the United Kingdon have implemented a three strikes type law, but it was demand side focused.[151]

---

[147] 156 CONG. REC. 126 (2010).

[148] S. 3804, 111th Cong. § 2(h)(2)(B) (2010).

[149] Rehberg v. Paulk, 611 F.3d 828, 843-44 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678, (U.S. 2011).

[150] Steve Tepp, *Chamber Responds to Center for Democracy and Technology's Comments Regarding the Leahy-Hatch Online Piracy Bill*, http://www.chamberpost.com/2010/09/chamber-responds-to-cdts-comments-regarding-the-leahy-hatch-online-piracy-bill/ (Sept. 28, 2010).

[151] Eldar Haber, *The French Revolution 2.0: Copyright and the Three Strikes Policy*, 2 Harv. J. Sports & Ent. L. 297, 299 (2011).

Senate Bill 3804 authorizes the Justice Department to demand an internet service provider to suspend the operation of the domain name for a website that features content violating copyright law.[152] Other countries such as Spain are also developing a "supply side" framework to combat pirated films on the net.[153] Instead, Spain has had a supply side graduated response program.[154] Perhaps the Spanish legislation (Law for a Sustainable Economy) will be further along in the future to allow for a robust analysis, but at this point it is too vague and generalized for us to take any lessons from it. In conclusion, at this point, the U.S. Bill, if made into law, would better protect against illegal file sharing originating from a website in Spain, than the Spanish legislation would.

France's Hadopi law offers little, if any, applicable insight. The French Hadopi (High Authority for the Distribution of Works and the Protection of Rights on the Internet)[155] focuses on the demand side.[156] The Hadopi law permits the "High Authority" (which is the regulating authority that the law creates), to basically label websites as legitimate because they are not trafficking in illegal content.[157] Similar to a government's stamp of approval, the list would encourage the public to use the websites listed and not the websites with pirated material, because it provides resources for people to turn if they are looking to access content on the web. However, there has not been much discussion of this issue in the law.[158] There is, however, French citizen involvement in the filtering policy against child pornography by '"tagging' sites for addition to a block list. . .French users can submit suspect sites, and the government then decides whether to include them

---

[152] S. 3804, 111th Cong. §2(e)(2)(B)(i) (2010).

[153] *The Spanish Government has further sharpened its assault on illegal file sharing*, PIRACY SNIPER, http://piracysniper.com/reduce_illegal_downloading_blog_files/2af6a4d5fb799992a1111a21b46d6ae6-23.html (Dec. 1, 2010).

[154] *Id.*

[155] Christian L. Castle, Amy E. Mitchell, *What's Wrong with ISP Music Licensing?*, 26 ENT. & SPORTS LAW 4, 6 (Fall 2008).

[156] *See generally* Nate Anderson, *French Anti-P2P Law Toughest in the World*, ARS TECHNICA, (Mar. 10, 2009), http://arstechnica.com/tech-policy/news/2009/03/french-anti-p2p-law-toughest-in-the-world.ars.

[157] *See* subsection 2, *Hadopi Full Translation,* http://www.laquadrature.net/wiki/HADOPI_full_translation.

[158] News Wires, *Top Legal Body Strikes Down Anti-Piracy Law*, FRANCE 24, (June 10, 2009), http://www.france24.com/en/20090610-top-legal-body-strikes-down-anti-piracy-law-hadopi-constitutional-council-internet-france.

on the list blocked by ISPs."[159] This community tagging system appears to be a positive step by creating a consumer approach to identifying and calling attention to illegal material.

It is particularly important to note the lack of supply-side international laws for two reasons. First of all, this means that this is relatively unchartered territory, so that the United States has no robust resource of laws. Secondly, and perhaps more importantly, the lack of such a law internationally justifies the Senate Bill even further, because Senate Bill 3804 would be the only effective response to global movie piracy on the web.

VIII. CONCLUSION

With more and more people seeking access to entertainment on the web, a secondary market for pirated films has developed online. With an economic toll on the entertainment industry reaching into billions of dollars, curbing infringing content on the web is not only good policy, it is a financial necessity. In order to prevent movie piracy from growing further and ideally to reduce its presence on the internet, it is important to look into effective solutions. The "Combating Online Infringement and Counterfeits Act" has been such an effort. By targeting the "supply-side" of the equation, it promises to take an innovative and efficient approach through targeting internet service providers, financial transaction providers, and advertisers. While Senate Bill 3804 is certainly a significant step in the right direction for targeting film piracy online, it is vital to consider policy implications and constitutional concerns to ensure that the Justice Department's efforts will be directed towards rooting out the illegal content and preserving material that the First Amendment protects.

Perhaps one of Senate Bill 3804's greatest assets is the ability it gives the Justice Department to sever the supply-side support of foreign websites, effectively shutting them down. This is a good example of how the U.S. legislation is tailored in a relatively narrow manner, since it would only involve foreign websites that target U.S. consumers with their pirated material. In analyzing the constitutionality of the amended Senate Bill 3804, this paper looked at the prior restraints as in *Nebraska Press Ass'n v. Stuart*, the Fourth and Fifth Amendment with such cases

[159] Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 401-02 (2009) (citing, *U.S., France Move to Block Online Child Pornography*, CBC NEWS (June 10, 2008), http://www.cbc.ca/technology/story/2008/06/10/isps-porn-block.html).

as *Rehberg v. Paulk* and *United States v. Ahrndt*, as well as cases such as *Viacom v. YouTube*, and *MGM v. Grokster, Ltd.* to balance the copyright holders and constitutional protections. The availability of infringing material on the web has made legislative intervention a necessity. Senate Bill 3804 may take the wind out of these movie pirates' sails.