Brooklyn Journal of International Law

Volume 30
Issue 3
SYMPOSIUM:
Intellectual Property Online: The Challenge of
Multi-Territorial Disputes

Article 11

2005

Filtering the Smoke Out of Cigarette Websites: A Technological Solution to Enforcing Judgments Against Offshore Websites

Michael Kwon

FILTERING THE SMOKE OUT OF CIGARETTE WEBSITES: A TECHNOLOGICAL SOLUTION TO ENFORCING JUDGMENTS AGAINST OFFSHORE WEBSITES

INTRODUCTION

Under the doctrine of international comity, the courts of most countries will enforce foreign judgments.[1] However, the borderless and global scope of the internet makes extraterritorial enforcement of a judgment against an offshore[2] website difficult because of the "internet's ability to cross borders, break down real world barriers, and destroy distance."[3] Under the internet's architecture, even determining the geographical location of internet users and content providers can prove difficult because the internet was initially designed to not disclose users' locations.[4] Thus, smaller actors who operate offshore websites can find both geographical and virtual safe havens[5] to avoid enforcement of judgments against them.[6]

To illustrate this problem, many cigarette websites operate overseas, making the enforcement of U.S. court judgments against them difficult.[7] In 2002, Philip Morris USA (Philip Morris) sued Otamedia, a cigarette website operator based in Switzerland, for violations of the Lanham Act[8] arising from

---

1. Mark D. Rosen, *Should "Un-American" Foreign Judgments Be Enforced?*, 88 MINN. L. REV. 783, 784 (2004).

2. For purposes of this Note, the term "offshore" means outside of U.S. territory.

3. *See* Matthew Fagin, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. TECH. L. REV. 395, 404 (2003), *available at* http://www.mttlr.org/volnine/Fagin.pdf (referring to the views of what the author terms "[internet] regulation critics" or "Internet separatists").

4. *Id*. at 404.

5. The term "safe haven" in this Note refers to either a real-world physical location or a virtual location where enforcing the law is difficult or impossible.

6. *See* Fagin, *supra* note 3, at 419 (arguing that smaller offshore actors can avoid enforcement of unilateral national regulation of the internet).

7. *Id*.

8. Lanham Act, 15 U.S.C. § 1114 (2000).

Otamedia's unauthorized sale of Philip Morris cigarettes over the internet.[9] Because Otamedia declined to answer Philip Morris's complaint, a default judgment was entered against Otamedia which enjoined it from selling cigarettes to U.S. consumers.[10] Otamedia ignored the default judgment by continuing to sell cigarettes to U.S. consumers over the internet, and the court modified its order and transferred Otamedia's U.S.-registered domain names,[11] yesmoke.com and yessmoke.com to Philip Morris.[12] However, both of these orders proved ineffectual because Otamedia found a virtual safe haven by registering new domain names, yesmoke.ch and yessmoke.ch, in Switzerland and thereby continued selling cigarettes to U.S. consumers from these domain names.[13] Even if Philip Morris eventually succeeds in obtaining Otamedia's Swiss domain names, hundreds of other cigarette websites still exist.[14] Thus, litigat-

9. Philip Morris USA, Inc. v. Otamedia Ltd., 331 F. Supp. 2d 228, 229 (S.D.N.Y. 2004).

10. *Id*.

11. A "domain name" is a user-friendly alphanumeric address for one or more computers connected to the internet used in lieu of a numeric address for such computers, called an IP address. *See* COMMITTEE TO STUDY TOOLS AND STRATEGIES FOR PROTECTING KIDS FROM PORNOGRAPHY AND THEIR APPLICABILITY TO OTHER INAPPROPRIATE INTERNET CONTENT, YOUTH, PORNOGRAPHY AND THE INTERNET § 2.1.5 (Dick Thornburgh & Herbert S. Lin eds., 2002) [hereinafter COMMITTEE]. "Registering a domain name" means that the domain name chosen will be associated with a designated computer on the internet. *See* ICANN, *Frequently Asked Questions*, *at* http://www.icann.org/faq/ (last visited May 23, 2005). A "registrant" is the person or entity that registers a domain name of its choosing and designates which computer will be associated with that domain name. *See id*. From that designated computer, the registrant can create a website which will be accessible to internet users around the world. *Id*. A registrant registers a domain name with a "registrar," an entity authorized to register domain names. *Id.* The registrar then transmits its registration information to a "registry," an entity that maintains all official records regarding registrations and implements the conversion from domain name to IP address. DAVID BENDER, COMPUTER LAW § 3D.05(3) (2004).

12. *Philip Morris*, 331 F. Supp. 2d at 247.

13. *See* Marton Dunai, *Altria Unit Wins Cigarette Vendor's Internet Address*, WALL ST. J., Aug. 25, 2004, at B2 [hereinafter Dunai, *Altria Unit*]; Adam Lisberg, *Feds Stub Out Big Cigs Racket*, N.Y. DAILY NEWS, Nov. 17, 2004, at 35.

14. *See* Patricia Sellers, *Altria's Perfect Storm*, FORTUNE MAG., Apr. 28, 2003, at 96 (in 2003, Philip Morris counted 536 cigarette websites); *see also* Philip Morris, *The Illicit Trade in Cigarettes: The Philip Morris International*

ing against each offshore cigarette website seems pointless when the website operators can simply flout U.S. court orders. The current structure of the domain name system (DNS)[15] makes seeking cigarette websites' domain names an impracticable remedy.[16] Therefore, rather than trying to reach offshore cigarette websites or their domain names extraterritorially, the better solution would be to limit access to these websites from within U.S. territory.[17]

The rapid development of filtering technology and its employment in enforcing online decency laws and court orders[18] indicates that the use of filtering technology to limit access of U.S. internet users to offshore cigarette websites may provide the most effective means of enforcing judgments against such websites without having to directly reach their conduct abroad.[19] The use of filtering technology has met with some approval from the U.S. Supreme Court,[20] Congress[21] and a French court[22] in the context of offensive content on websites. Furthermore,

---

Perspective, at 9 (2004), *available at* http://www.philipmorrisinternational.com /global/downloads/OBE/Illicit_trade.pdf ("As of January 2004, there are literally hundreds of internet websites offering to sell tobacco products of every imaginable description.").

15. The "domain name system" refers to the internet naming system that translates numeric IP addresses of computers connected to the internet into an easier-to-remember alphanumeric domain name. *See* COMMITTEE, *supra* note 11, § 2.3.1.

16. *See infra* Part II.

17. *See infra* Part IV.

18. *See infra* Part III.

19. *See infra* Part IV.

20. *See* Ashcroft v. ACLU, 124 S. Ct. 2783, 2792 (2004) (finding filtering technologies less restrictive on protected speech than the Child Online Protection Act which criminalizes the posting of content on the internet that is harmful to children).

21. Congress declared that it is the policy of the United States "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4) (2000). Also, Congress passed the Children's Internet Protection Act, which requires libraries to use filtering technology to block obscene material as a condition to receiving federal funds. 47 U.S.C. § 254(h)(6)(B)(i) (2000).

22. *See* UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, Nov. 22, 2000, obs. J. Gomez, *translated in* http://www.cdt.org/speech/international/ 001120yahoofrance.pdf [hereinafter Yahoo *II*] (finding filtering technology a feasible remedy to block French users from viewing Nazi memorabilia).

the use of filtering technology to prevent only U.S. users from accessing websites that infringe Philip Morris's trademark is consistent with the territoriality principle of trademark law.[23]

Part I of this Note explores the rise of cigarette websites and Philip Morris's challenges against them, in particular against Otamedia. Part II analyzes how the current structure of the DNS makes Philip Morris's remedy of obtaining domain names an ineffectual means of enforcing judgments against offshore websites that seek safe havens in bad faith. Part III reviews two prior government-mandated uses of filtering technology, one by a French court ordering Yahoo! to block French users from accessing illegal Nazi memorabilia on Yahoo's auction site, and another by internet service providers (ISPs)[24] in Pennsylvania to comply with a state child pornography statute. Part IV proposes a method of implementing a filtering technology regime at the level of domestic ISPs as a fair and efficient means of enforcing judgments against offshore websites when reaching their conduct extraterritorially proves difficult or impossible.

I. THE RISE OF CIGARETTE WEBSITES

In recent years, the retail price of cigarettes in the United States has increased dramatically.[25] Between 1997 and 2002, the average price of cigarettes in the United States rose ninety percent.[26] In part, this price increase can be attributed to higher taxes on cigarettes.[27] Since 2002, twenty-nine states and the District of Columbia have increased their cigarette excise taxes,[28] bringing the national average to sixty-five cents per

23. As a general rule, trademark rights do not extend beyond the territory of a nation. *See* Paris Convention for the Protection of Industrial Properties, July 14, 1967, art. 6(3), 21 U.S.T. 1583 ("A mark duly registered in a country of the Union shall be regarded as independent of marks registered in the other countries of the Union, including the country of origin.").

24. An ISP is a company which provides other companies or individuals with access to, or presence on, the internet. *See* Dictionary.com, *at* http://dictionary.reference.com/search?q=internet+service+provider.

25. *See* Sellers, *supra* note 14, at 96.

26. *Id*.

27. *See* Noam Neusner, *Tobacco is Becoming the Smuggler's Choice*, U.S. NEWS & WORLD REPORT, Nov. 4, 2002, at 46.

28. John Berlau, *Smoking Out Big Tobacco*, INSIGHT ON THE NEWS, Nov. 25, 2003, at 18.

pack.[29] Taxes constitute approximately sixty percent of the total price of cigarettes.[30] The recent price increase of cigarettes can also be attributed to civil judgments rendered against the tobacco industry.[31] The tobacco industry has shifted the cost of its liability for the harmful effects of cigarettes to its consumers.[32] For instance, in 1998, the state attorneys general settled their Medicaid reimbursement lawsuits against the major tobacco companies[33] who agreed to pay the states $254 billion over twenty-five years.[34] According to a tobacco analyst, the tobacco companies' payments to the states increased the cost of cigarettes by fifty-six cents per pack.[35]

With the rising price of cigarettes in the United States, some consumers have turned to the internet to take advantage of lower prices.[36] To illustrate the price advantage of buying cigarettes over the internet, in New York City, a carton of cigarettes can cost upwards of seventy dollars,[37] while a carton of cigarettes over the internet can cost less than fifteen dollars.[38] As of 2003, internet sales of cigarettes accounted for a little more

---

29. John Reid Blackwell, *Tobacco Campaign: Major Companies Defend their Turf Against 'Underground' Competitors*, RICHMOND TIMES DISPATCH, Mar. 24, 2003, at D4. In 2002, the states with the highest taxes per pack of cigarettes were: New York ($1.50), New Jersey ($1.50), Washington ($1.425), Rhode Island ($1.32), and Hawaii ($1.20). Neusner, *supra* note 27, at 46.

30. Berlau, *supra* note 28, at 18.

31. *See* Sellers, *supra* note 14, at 96.

32. *Id*.

33. The tobacco companies involved in the settlement were Philip Morris Cos., R.J. Reynolds Tobacco Co., Lorillard Inc., and Brown & Williamson Tobacco Corp. Heather MacGregor & Matt Ackerman, *Judge Approves States' $7.6B Share of $206B Pact with Tobacco Industry*, N.J. L.J., Dec. 7, 1998, at 822.

34. Neusner, *supra* note 27, at 46. The 1998 settlement involved all fifty states. *See* MacGregor & Ackerman, *supra* note 33, at 822. Four states settled individually while the remaining forty-six states settled for a tobacco industry payment of $206 billion over twenty-five years beginning on April 15, 2000. *Id*. In the settlement, Philip Morris agreed to pay half of the $254 billion settlement. Sellers, *supra* note 14, at 96.

35. Neusner, *supra* note 27, at 46.

36. Blackwell, *supra* note 29, at D4 ("Hundreds of web sites have sprung up to cater to customers who are fed up with high cigarette prices.").

37. Marton Dunai, *Duty-Free Web Site's Cigarette Sales Ignite U.S. Scrutiny*, WALL ST. J., Aug. 5, 2004, at B1 [hereinafter Dunai, *Duty-Free*].

38. Dunai, *Altria Unit*, *supra* note 13, at B2.

than two percent of total cigarette sales in the United States.[39] That figure has been estimated to reach fourteen percent by 2005.[40] According to Philip Morris, as of January 2004, hundreds of websites sell cigarettes over the internet.[41] Cigarette websites obtain discounted cigarettes in several ways.[42] Some websites operate from Indian reservations and are able to sell discounted cigarettes because they are exempt from state and federal excise taxes.[43] Other websites operate from states with low cigarette taxes[44] or operate offshore.[45] Many, if not all, of these offshore websites can sell cigarettes at much lower prices than local retailers because the cigarettes they sell are either counterfeit[46] or "gray market," which are cigarettes manufactured for sale overseas but are re-imported and sold without the manufacturer's permission.[47] Offshore cigarette websites often remove the cigarettes from their original packaging and disguise them in "book format" to avoid detection by customs agents.[48]

The rise of internet cigarette sales has drawn the attention of both state and federal governments.[49] Connecticut Attorney

39. Philip Morris, *supra* note 14, at 9; *see also* Blackwell, *supra* note 29, at D4.

40. Neusner, *supra* note 27, at 46.

41. Sellers, *supra* note 14, at 96.

42. *See* Blackwell, *supra* note 29, at D4.

43. Sellers, *supra* note 14, at 96.

44. Blackwell, *supra* note 29, at D4.

45. *See generally* Dunai, *Duty-Free*, *supra* note 37, at B1 (describing the operations of Otamedia in Switzerland).

46. The Organisation for Economic Co-operation and Development defines "counterfeit" as "a product which so closely imitates the appearance of the product of another to mislead a consumer that it is the product of another. Hence, it may include trademark infringing goods, as well as copyright infringements [and] includes copying of packaging, labeling and any other significant features of the product." Organisation for Economic Co-operation and Development, *The Impact of Counterfeiting*, at 3 (1998), *available at* http://oecd.org/dataoecd/11/11/2090589.pdf.

47. Blackwell, *supra* note 29, at D4. "Gray market" cigarettes also refer to surplus cigarettes manufactured overseas then imported and sold at a deep discount. *See* Dunai, *Duty-Free*, *supra* note 37, at B1.

48. Philip Morris, *supra* note 14, at 9. This report also provides photographs of cigarettes repackaged in "book format." *Id*.

49. *See*, *e.g.*, Jim VandeHei, *GOP Whip Tried to Aid Big Donor; Provision was Meant to Help Philip Morris*, WASH. POST, June 11, 2003, at A01 (Congressional attempt to make it harder to sell cigarettes online); David Pittman,

General Richard Blumenthal stated that "[i]nternet tobacco sales outlets almost never make a meaningful effort to enforce age restrictions."[50] In addition to the problem of minors obtaining cigarettes online, the states lost an estimated $552.4 million in tax revenue because of illegal cigarette sales in 2003.[51] The loss of tax revenue and the ease of minors obtaining cigarettes online have prompted some states to pass statutes designed to curb the sale of cigarettes online.[52] In 2000, New York State enacted a statute[53] that outright bans internet cigarette sales by prohibiting cigarette sellers and carriers from shipping and transporting cigarettes directly to New York consumers.[54] In 2004, Kansas passed a statute[55] that regulates internet cigarette sales by requiring cigarette shippers to register with the state as retailers, collect sales tax, remit the taxes to the state, and buy cigarette tax stamps from the state.[56] The Kansas law also addresses the problem of underage purchases of cigarettes online by requiring sellers to obtain certifications from purchasers that they are of legal age and that the cigarettes are not in-

---

Ariz. Gunning for Buyers of Online Smokes, TUCSON CITIZEN, Aug. 26, 2004, at 1D (Arizona law imposes fines on internet cigarette purchasers); John Petterson, *Cigarette Tax Measure Focus of Ceremony*, KANSAS CITY STAR, June 16, 2004, at 3 (Kansas law designed to discourage online cigarette sales); Tom Wanamaker, *Seneca Nation Sues New York over Internet Smoke-Sales Ban*, INDIAN COUNTRY TODAY, Jan. 28, 2004, *available at* http://www.indiancountry.com/content.cfm?id=1074965057 (New York State bans online cigarette sales); Staff and Wire Reports, *MD Atty. General Reached Settlement with Internet Cigarette Retailers*, DAILY RECORD, Dec. 4, 2003, *available at* http://www.findarticles.com/p/articles/mi_qn4183/is_200312/ai_n10059248 (Maryland sued internet cigarette retailer for tax evasion and sale to minors); Richard Blumenthal, *Tobacco Control: A State Perspective*, 3 YALE J. HEALTH POL'Y L. & ETHICS 151, 154 (2003) (Connecticut Attorney General and Department of Revenue Services created a task force to combat online cigarette sales).

50. Blumenthal, *supra* note 49, at 154.

51. Pittman, *supra* note 49, at 1D.

52. *See id*.

53. Unlawful Shipment or Transport of Cigarettes, N.Y. PUBLIC HEALTH LAW § 1399-ll (McKinney 2004).

54. Brown & Williamson Tobacco Corp. v. Pataki, 320 F.3d 200, 202 (2d Cir. 2003).

55. Sale of Cigarettes; Requirements; Internet, Telephone or Mail Order Transactions, Requirements; Packages of Cigarettes; Penalties, 2004 Kan. Sess. Laws Ch. 140 § 1 (2004).

56. Petterson, *supra* note 49, at 3.

tended for use by a minor.[57] A new Arizona statute[58] requires internet sellers to file monthly reports with the state listing the names, ages, addresses, and purchases of customers and to verify that they have collected all state taxes owed.[59] Violation of the law by sellers or shippers could result in criminal felony prosecution and fines up to $5,000 or five times the price of cigarettes purchased, whichever is greater.[60] Washington and California have similar laws regulating online cigarette sales.[61]

The federal government has also addressed the problem of internet cigarette sales.[62] In 2000, Congress passed the Imported Cigarette Compliance Act[63] which bans the reimportation of cigarettes bearing a U.S. trademark without the consent of the trademark holder.[64] The U.S. Senate has passed the Prevent All Cigarette Trafficking Act (PACT Act),[65] which would make it easier for federal law enforcement to combat the importation of cigarettes via the internet by reducing the number of cigarettes necessary to make interstate smuggling a fed-

57. *Id*.

58. Cigarettes; Delivery Sales, 2004 Ariz. Sess. Laws Ch. 311, SB1353 (2004), *available at* http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/legtext/46leg/2r/laws/0311.htm.

59. Pittman, *supra* note 49, at 1D.

60. *Id*.

61. *Id*.

62. *See*, *e.g.*, VandeHei, *supra* note 49, at A01.

63. 19 U.S.C. §§ 1681–1681b (2000).

64. *Id*. According to a Philip Morris spokesperson, Philip Morris has sued seven cigarette websites operating overseas under this Act and has won six of those suits. Michael Bobelian, *Pursuing Counterfeiters: Litigation is One Option to Stop Sales of Fake Products*, N.Y. L.J., Oct. 14, 2004, at 5. Under 19 U.S.C. § 1681a(a)(4) (2000), "[C]igarettes may be imported into the United States only if … such cigarettes bear a United States trademark registered for such cigarettes [and] *the owner of such United States trademark registration for cigarettes … has consented* to the importation of such cigarettes into the United States" (emphasis added). Philip Morris, a U.S. trademark owner, asserts that it does not consent to the sale of its brands over the internet because many of them lack age verification, encourage consumers to evade taxes, sell cigarettes intended for one country that do not comport with warning label requirements in the country where they are ultimately sold, violate advertising laws, falsely imply affiliation with Philip Morris, sell counterfeit cigarettes, and take consumers' credit card information but fail to deliver the cigarettes ordered. Philip Morris, *supra* note 14, at 9. According to Philip Morris officials, Philip Morris has *never* authorized internet sales of its brands. Blackwell, *supra* note 29, at D4.

65. S. 1177, 108th Cong. (2003).

eral crime from 60,000 to 10,000.[66] The House of Representatives has yet to pass the PACT Act.[67] The House is also reviewing an amendment to the Jenkins Act,[68] tentatively called the Internet Tobacco Sales Enforcement Act.[69] The amendment, if signed into law, would regulate interstate online cigarette sales and would make it harder for cigarette websites to evade taxes.[70]

In 2003, House Representative Roy Blunt attempted to insert a provision in the Homeland Security Bill that would have made it harder to sell cigarettes over the internet.[71] Representative Blunt had instructed congressional aides to add the provision to the bill within hours of the final House vote without anyone in the House either supporting the provision or aware of its last-minute addition into the Homeland Security Bill.[72] However, Speaker J. Dennis Hastert's chief-of-staff was alerted to the provision and had it pulled before the final House vote, ultimately thwarting Representative Blunt's secret attempt to add the provision.[73] The attempt to add the tobacco provision became a scandal for Representative Blunt because he had re-

66. William V. Corr, *Campaign for Tobacco-Free Kids: Federal and State Governments Must Strengthen Efforts to Combat Cigarette Smuggling*, U.S. NEWSWIRE, June 9, 2004, *available at* http://releases.usnewswire.com/GetRelease.asp?id=31717.

67. *See id*.

68. Jenkins Act, 15 U.S.C. § 375 (2000). This statute regulates mail-order trade. Dunai, *Duty-Free*, *supra* note 37, at B1.

69. H.R. 2824, 108th Cong. (2004). Section 2 of the bill reads in pertinent part:

> Each person who engages in an *interstate sale of cigarettes or smokeless tobacco* … shall comply with all the excise, sales, and use tax laws applicable to the sale or other transfer of cigarettes or smokeless tobacco in the State and place in which the cigarettes or smokeless tobacco are delivered as though the person were physically located in that State or place.

H.R. 2824 § 2, 108th Cong. (2004) (emphasis added). The term "interstate sale of cigarettes or smokeless tobacco" is defined as "any sale of cigarettes or smokeless tobacco in interstate or *foreign commerce*." H.R. 2824 § 7(4) (2004) (emphasis added). Thus, if the bill were signed into law, offshore cigarette websites would be required to comply with *all* taxes applicable to the sale as though the websites were physically located in that state.

70. Dunai, *Duty-Free*, *supra* note 37, at B1.

71. VandeHei, *supra* note 49, at A01.

72. *Id*.

73. *Id*.

ceived large campaign donations from Philip Morris, a major campaign contributor and lobbying force on Capitol Hill,[74] and because his son and wife were lobbyists for Philip Morris.[75] Representative Blunt argued that the provision was relevant to homeland security because terrorist groups such as Hezbollah[76] allegedly profited from the sale of contraband cigarettes.[77] However, a representative for Altria Group, the parent company of Philip Morris, admitted that the tobacco provision was "pretty important to [them]."[78] In fact, Philip Morris has also been lobbying in state legislatures for more restrictions on cigarette websites.[79] Philip Morris wants legislation curbing the sale of its cigarette brands over the internet because such sales have been a contributing factor to the company's declining profits in recent years.[80]

Philip Morris's efforts to curb the sale of cigarettes over the internet has not been limited to lobbying legislatures.[81] In 2002, Philip Morris established its "Brand Integrity Department," which was designed to collect intelligence and combat the illegal sale of Philip Morris cigarette brands, such as counterfeit cigarettes, smuggled cigarettes, internet sales, and imported gray

74. Juliet Eilperin, *Lobbyist Curbs Role Over Tie to Rep. Blunt*, WASH. POST, Sept. 9, 2003, at A21.

75. Berlau, *supra* note 28, at 18.

76. Hezbollah is a Lebanese terrorist group of Shiite militants. Council on Foreign Relations, *Terrorism: Q & A*, *at* http://www.cfrterrorism.org/groups/hezbollah.html. A group of more than two dozen men bought cigarettes in North Carolina where the taxes were fifty cents per carton, resold them in Michigan where taxes were $7.50 per carton, then sent their profits to Hezbollah. Neusner, *supra* note 27, at 46.

77. VandeHei, *supra* note 49, at A01. The terrorist ties to illegal cigarette sales does not end there. In 1993, the group convicted of planning the first World Trade Center attack possessed counterfeit cigarette tax stamps. Neusner, *supra* note 27, at 46. Also, Saddam Hussein's son, Udah, allegedly oversaw a cigarette-smuggling operation in Iraq, "primarily to enrich his family and fund Iraq's weapons programs." *Id*.

78. VandeHei, *supra* note 49, at A01.

79. Blackwell, *supra* note 29, at D4.

80. Sellers, *supra* note 14, at 96 (reporting that in 2002 Philip Morris saw profits fall thirteen percent from the previous year primarily because the rising cost of cigarettes has resulted in smokers finding better bargains from websites, deep-discount brands, and counterfeit cigarettes).

81. *See generally* Blackwell, *supra* note 29, at D4 (describing various efforts by Philip Morris to combat the sale of counterfeit and gray market cigarettes).

market cigarettes.[82] The Brand Integrity Department works to complete much of the investigatory work itself before handing off cases to law enforcement.[83] To this end, Philip Morris staffed its Brand Integrity Department with former law enforcement experts from the Secret Service, Customs, the Bureau of Alcohol Tobacco Firearms and Explosives, and the FBI.[84] The department also consists of Philip Morris employees with expertise in distribution channels, packaging and design.[85]

Beginning in 2002, Philip Morris brought twenty lawsuits against sixty-seven online cigarette vendors.[86] The lawsuits allege that the cigarette websites violate the Lanham Act[87] by misusing Philip Morris's trademarks in an effort to attract internet users to their sites and that the websites are selling cigarettes that have been imported in violation of the Imported Cigarettes Compliance Act of 2000.[88] Philip Morris has been successful in almost every case that has been decided, including one against Otamedia, the operator of the website Yesmoke.com.[89] The suit against Otamedia provides the perfect example of how ineffectual both state and federal governments as well as Philip Morris have been in curbing the sale of gray market or counterfeit cigarettes by offshore websites.[90]

The owners of Otamedia, Italian brothers Gianpaolo and Carlo Messina,[91] first incorporated Otamedia in the Isle of Man, and later in Belize, and presently operate from Switzerland.[92]

---

82. *Id*.

83. Bobelian, *supra* note 64, at 5.

84. *Id*.

85. *Id*.

86. Dunai, *Altria Unit*, *supra* note 13, at B2. In addition to Otamedia, the cigarette websites that Philip Morris has sued include: allsmoke.com, cheapmarlboro.com, discountcigs.homestead.com, discountcigarettes.cjb.net, europecigarettes.com, freefags.com, smokefarm.com, smokeplanet.com, smoke.shop4all.net, and 18orless.com. *Philip Morris Sues Internet Vendors*, NAT'L PETROLEUM NEWS, Nov. 1, 2002, at 7.

87. 15 U.S.C. § 1114 (2000).

88. *Philip Morris Sues Internet Vendors*, NAT'L PETROLEUM NEWS, Nov. 1, 2002, at 7.

89. The website now operates under the domain names yesmoke.ch or yessmoke.ch. Dunai, *Duty-Free*, *supra* note 37, at B1.

90. *See*, *e.g.*, Bobelian, *supra* note 64, at 5.

91. *See* Dunai, *Duty-Free*, *supra* note 37, at B1.

92. *Philip Morris*, 331 F. Supp. 2d at 229 n.1.

The Otamedia website has drawn millions of customers.[93] After establishing Otamedia in 2000, the Messina brothers said they quadrupled their revenue to $80 million in 2003 and expected to generate over $100 million in 2004.[94] Otamedia registered its domain names, yesmoke.com and yessmoke.com, with Network Solutions Inc., a domain name registrar located in Virginia.[95] The website attracts customers by using "metatags," invisible strings of keywords that include: "Marlboro," "Camel" and other cigarette brands, as well as "cigarettes," "online" and "duty-free."[96] Internet users who enter these keywords into a search engine are directed to Otamedia's website.[97] On the website's homepage, the byline "Your online cigarette store" appears above a picture of a man wearing an Alpine hat lighting a cigarette that resembles the silhouette icon of the "Marlboro Man."[98] Previously, the website displayed a picture that resembled the Marlboro Man even more closely, wearing a cowboy hat rather than the Alpine hat now worn,[99] perhaps to mislead consumers into believing the site is affiliated with Philip Morris. In addition to selling cigarettes, the website also posts articles about tobacco-related news, tobacco safety, and editorials denouncing Philip Morris.[100]

According to Carlo Messina, Otamedia obtains its cigarettes from several sources.[101] Otamedia buys its cigarettes in bulk

93. Dunai, *Altria Unit*, *supra* note 13, at B2.
94. Dunai, *Duty-Free*, *supra* note 37, at B1.
95. Dunai, *Altria Unit*, *supra* note 13, at B2.
96. Dunai, *Duty-Free*, *supra* note 37, at B1.
97. *Id*.
98. *Philip Morris*, 331 F. Supp. 2d at 235.
99. *Id*. at 235 n.9.
100. For example, after Philip Morris filed its order to show cause seeking the transfer of Otamedia's domain names, Otamedia responded by posting on its website, "This is what can happen when the colossus [i.e. Philip Morris] decides to impose itself on someone: this is how it intimidates without making threats, how it isolates its enemies without committing any criminal act. The PM company, in fact, tries to conquer using clichés and people's fears." Otamedia, *"A Close Encounter" with the Multinational Company*, *at* http://www.yesmoke.ch/news/pmvy/020915.php. After the court ordered the transfer of Otamedia's ".com" domain names to Philip Morris, Otamedia posted on its website that "Philip Morris shows itself to be a rotten merchant that treads on the rights of American citizens." Otamedia, *The Virtual Victory of Big Tobacco*, *at* http://www.yesmoke.ch/news/pmvy/040819.php.
101. Dunai, *Duty-Free*, *supra* note 37, at B1.

from duty-free chains and a Dutch clearinghouse.[102] The Messina brothers also claim that their cigarettes come from a Philip Morris factory in the Philippines that sells its surplus at a deep discount.[103] However, Philip Morris officials deny that their factories directly supply Otamedia and assert that the cigarettes are probably counterfeit.[104] The cigarettes arrive at and leave from a duty-free customs haven in Switzerland where Otamedia can avoid paying Swiss taxes or customs because the cigarettes never formally enter Switzerland.[105]

Philip Morris, as part of its effort to curb the unauthorized online sale of its brands, sued Otamedia in 2002.[106] Philip Morris sought declaratory and injunctive relief for trademark infringement, unfair competition, and other violations of the Lanham Act[107] and analogous state law, arising from Otamedia's unauthorized sale of Philip Morris cigarettes over the internet.[108] Otamedia declined to answer Philip Morris's complaint,[109] and the court therefore entered a default judgment against

---

102. *Id*.
103. *Id*.
104. *Id*.
105. *Id*.
106. *Philip Morris*, 331 F. Supp. 2d at 229.
107. 15 U.S.C. § 1114 (2000) reads in pertinent part:

> Any person who shall, without the consent of the registrant … use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive . . . shall be liable in a civil action by the registrant for the remedies hereinafter provided.

Id.

108. *Philip Morris*, 331 F. Supp. 2d at 229.
109. According to Otamedia, it decided not to answer the complaint because Philip Morris demanded lists of all of Otamedia's suppliers and customers, the names of its employees, and the company's balances. Otamedia claimed that disclosing such information would be "a serious crime for [sic] Swiss law." Otamedia, *"A Close Encounter" with the Multinational Company*, *at* http://www.yesmoke.ch/news/pmvy/020915.php. However, Otamedia's lawyers felt obligated to comply with the discovery demand, so Otamedia "abandoned both the suit and the lawyers." *Id*. On the other hand, "Otamedia may well have calculated that the Judgment itself posed no threat to its business, given the obstacles to enforcing it in any meaningful way against a foreign entity." *Philip Morris*, 331 F. Supp. 2d at 234 n.6.

Otamedia on January 27, 2003.[110] The default judgment enjoined Otamedia from using Philip Morris's trademarks and from supplying cigarettes, fulfilling orders for drop shipping, or facilitating the importation of gray market Philip Morris cigarettes into the United States.[111]

Despite the court order, the Messina brothers continued selling gray market cigarettes to U.S. consumers.[112] This began a series of cat-and-mouse maneuvers between Philip Morris and Otamedia.[113] Several months after the default judgment, Otamedia's staff discovered a jumble of wires and electronics in a box of L&M cigarettes.[114] Thinking it was a bomb, many Otamedia employees fled the scene.[115] Otamedia received five more wired boxes, which turned out to be not bombs, but tracking devices planted by Philip Morris, which wanted to find out how Otamedia obtains its cigarettes.[116]

Realizing that the court order enjoining Otamedia from selling cigarettes to U.S. consumers proved wholly ineffectual, on August 4, 2003, Philip Morris brought an order to show cause, which sought to modify the default judgment by a court order to transfer ownership of the U.S.-registered domain names, yesmoke.com and yessmoke.com, to Philip Morris.[117] In response, Otamedia registered new domain names, yesmoke.ch and yessmoke.ch, in Switzerland and automatically redirected visitors to

---

110. *Philip Morris*, 331 F. Supp. 2d at 229. The default judgment found:

> The Otamedia Website displays logos and images confusingly similar to those of Philip Morris trademarks [citation to judgment omitted], and through it, Otamedia illegally sells to customers in the United States Philip Morris cigarettes intended for sale abroad ("gray market cigarettes"). The Otamedia Website also infringes and dilutes Philip Morris trademarks, violates both the Imported Cigarette Compliance Act, 19 U.S.C. § 1681 *et seq.* and New York General Business Law § 360-1, and constitutes false advertising and unfair competition under the Lanham Act.

Id. Because Otamedia defaulted, the court found the facts in Philip Morris's complaint admitted by Otamedia. *Id*.

111. *Id*.

112. *Id*. at 246–47.

113. Dunai, *Duty-Free*, *supra* note 37, at B1.

114. *Id*.

115. *Id*.

116. *Id*.

117. *Philip Morris*, 331 F. Supp. 2d at 229.

its new ".ch" domain names before the order to show cause could be adjudicated.[118] Otamedia also registered other new domain names that redirected internet users to the Otamedia website, including yespeedy.com, yesspeedy.com, yes-speedy.ch, and otamedia.com.[119] In response, Philip Morris filed subsequent submissions, which asked the court to include Otamedia's new Swiss domain names in the order to show cause.[120] However, because Philip Morris did not request this relief in its initial motion papers and had not established an adequate legal or factual basis for it, the court denied the request without prejudice, which left open the possibility that the court will order the transfer of Otamedia's Swiss domain names in the future.[121]

On August 20, 2004, the court found that Otamedia violated the default judgment by devoting its business almost exclusively to selling gray market cigarettes, a substantial percentage of which were Philip Morris brands, to U.S. consumers.[122] The court therefore ordered that the domain names yes-

118. *Philip Morris*, 331 F. Supp. 2d at 234 n.8. "The '.ch' extension signifies that the domain name is registered in Switzerland; 'ch' stands for *Confederation Helvetique*." *Id.*

119. *Id*.

120. *Id*. at 231 n.3. The transfer of domain names is the typical remedy for cybersquatting claims, which hold a person liable who in bad faith intended to profit from a protected trademark and "registers, traffics in, or uses a *domain name* that . . . is identical or confusingly similar to or dilutive of that mark." Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)(1)(A)(ii)(II) (2000) (emphasis added). However, Otamedia's infringement of Philip Morris's trademark was not in its domain names because "yesmoke.com" or "yessmoke.com" are not "identical or confusingly similar to or dilutive of that mark." Rather, the trademark infringement occurred on the content of the website itself in that it displayed "logos and images confusingly similar to those of Philip Morris trademarks." *Philip Morris*, 331 F. Supp. 2d at 229. This is not to say that such a remedy must be limited to cybersquatting claims.

121. *Philip Morris*, 331 F. Supp. 2d at 231 n.3.

122. *Id*. at 244. Unlike the initial complaint, Otamedia opted to appear in court for the order to show cause. Carlos Messina, the co-owner of Otamedia with his brother Gianpaolo Messina, filed a declaration with the court describing himself as the "Director of the Legal Department for Otamedia Limited." *Id*. at 231. However, he later testified that Otamedia does not have a specific legal office or department but that he is the one in charge of it. *Id*. at 231 n.3. At the evidentiary hearing for the order to show cause, the court found that Messina produced fabricated evidence and may have perjured himself. *Id*. at 245, 247.

moke.com and yessmoke.com be transferred to Philip Morris.[123] Addressing the difficulty of enforcing judgments against offshore websites, the court stated that "[b]efore this proceeding, Otamedia evidently calculated that its elusive and ephemeral location, coupled with the 'virtual' nature of its business, placed it safely beyond the reach of conventional enforcement measures available to a U.S. federal court."[124] The court found that the remedy of transferring Otamedia's U.S.-registered domain names to Philip Morris would be "an *efficacious* means to enforce the Judgment, a means inherent in the very same technology by which Otamedia has to date been able to violate it with impunity."[125]

However, merely transferring Otamedia's U.S.-registered domain names, but not its Swiss-registered domain names, proved to be a wholly *inefficacious* means of enforcing the judgment because U.S. consumers continue buying cigarettes from Otamedia through its Swiss-registered domain names.[126] This ruling constitutes the second "victory" of Philip Morris against Otamedia in U.S. courts.[127] Jack Holleran, the senior

123. *Id*. at 247.

124. *Id*. at 245.

125. *Id.* (emphasis added).

126. On November 16, 2004, agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) seized tons of cigarettes at John F. Kennedy Airport which were shipped to the United States by Otamedia. Lisberg, *supra* note 13, at 35. This occurred almost three months after Philip Morris seized Otamedia's U.S.-registered domain names, proving that the order did nothing to enjoin Otamedia from selling cigarettes to U.S. consumers. However, after the ATF seizure of Otamedia's shipment, Otamedia posted on its website, "because of our recent problems at New York's J.F.K. Airport, we have, against our will, been obliged to interrupt our regular shipments to the United States. We plan to start selling Yesmoke cigarettes in the States on January 2005." Otamedia, *Letter to its U.S. Consumers*, *at* http://www.yesmoke.ch/communicate.php.

127. The first "victory" was the default judgment rendered on January 27, 2003. *See Philip Morris*, 331 F. Supp. 2d at 229. Otamedia's litigation woes did not end with this case. On October 13, 2004, New York City won a $17,382,121 judgment against Otamedia. Carl Campanile, *$17M Fine Burns 'Net Cig Seller*, N.Y. POST, Oct. 13, 2004, at 4. The City alleged that Otamedia misled consumers into believing they could evade tobacco taxes by buying cigarettes online. *Id*. Like its initial suit against Philip Morris, Otamedia repeatedly failed to respond to court papers or to appear in court. *Id*. City lawyers assert that the judgment is the largest against a contraband cigarette scam to date. *Id*. Eric Proshansky, a lawyer for New York City, stated that

vice president of Philip Morris's Brand Integrity Department, stated after the ruling, "We are pleased Judge Lynch has ordered … continued protection of our trademark rights. We believe this will send a message to all Internet retailers who sell our products unlawfully."[128] However, the real message being sent by this ruling is that if a website operates from and registers its domain name outside the United States, then U.S. courts have no effective means of enforcing judgments against it.

II. SEIZING THE DOMAIN NAME: AN INEFFECTUAL REMEDY

Philip Morris's attempt to enjoin Otamedia's unauthorized sale of Philip Morris brands by seizing its domain names can be analogized to New York City's padlocking of unlicensed cigarette retailers' physical premises when the retailer violates the city's order to cease the unlicensed activity.[129] Otamedia's domain names are the virtual doors of its online cigarette store and Philip Morris is essentially trying to padlock its doors.[130] This analogy highlights the problem of combating offshore internet cigarette dealers: while New York City is able to exercise physical control over its cigarette retailers within city limits, Philip Morris has not been able to exercise virtual control over offshore internet cigarette dealers.[131] After Philip Morris obtained Otamedia's U.S.-registered domain names, the Otamedia website posted its reaction to the decision by stating, "Yesmoke can continue to sell from its Swiss domain to its customers all over the world…because Philip Morris has never made any move against the Yesmoke.ch site, as this would re-

---

"[Otamedia is] an elusive company . . . . We'll find out where they are and collect the judgment." *Id*.

128. Dunai, *Altria Unit*, *supra* note 13, at B2.

129. New York City Administrative Code § 20-105(b)(3) (1986), also referred to as the "padlock law," authorizes the Commissioner of the Department of Consumer Affairs, after notice and a hearing, to order that the premises on which unlicensed activity is occurring be sealed. *Id*.

130. "[A] domain name can be likened to . . . opening the door to a place of business." Jason Berne, *Court Intervention but not in a Classic Form: A Survey of Remedies in Internet Trademark Cases*, 43 ST. LOUIS U. L.J. 1157, 1170 (1999). "[T]he domain name is the gateway to the products or services offered." David Romero, *A Worldwide Problem: Domain Name Disputes in Cyberspace Who is in Control?*, 9-Sum CURRENTS: INT'L TRADE L.J. 69, 73 (2000).

131. *See supra* Part I.

quire the ruling of a Swiss judge."[132] Indeed, because of the currently fractured structure of the DNS, seeking domain names registered abroad may require litigating in the country where the domain name is registered. To understand why, a basic description of the DNS may be helpful.

The "internet" is essentially a giant network of computers.[133] Each computer comprising a part of the internet has a unique identifying number, called an internet protocol address (IP address).[134] An IP address consists of four groups of digits separated by a period.[135] The DNS was developed as a user-friendly approach to surfing the internet without having to remember numeric IP addresses to find a particular website.[136] The DNS consists of a directory of all the domain names and their corresponding IP addresses.[137] Under the DNS, each IP address contains one or more unique alphanumeric domain names.[138] Thus, users can type in a domain name, such as "amazon.com," instead of a long and difficult-to-remember numeric IP address, to find a particular website.[139] When a domain name is entered into the location box of an internet browser, the user's computer determines the website's corresponding IP address.[140] A domain name consists of alphanumeric strings separated by a dot.[141] The string of characters preceding the dot is called the second level domain.[142] The designation following the dot is called the

132. Otamedia, *The Virtual Victory of Big Tobacco*, *at* http://www.yesmoke.ch/news/pmvy/040819.php (Aug. 19, 2004).

133. *See* BENDER, *supra* note 11, § 3D.05(1).

134. *Id*.

135. Romero, *supra* note 130, at 69. For example, an IP address might be "123.45.678.90."

136. *See* Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 195 (2000).

137. ICANN, *Frequently Asked Questions*, *at* http://www.icann.org/faq/ (last visited May 23, 2005).

138. Through a process called IP-based virtual hosting, multiple domain names can be assigned to the same IP address. COMMITTEE, *supra* note 11, § 2.3.1.

139. *See* BENDER, *supra* note 11, § 3D.05(1).

140. Kim G. von Arx & Gregory Hagen, *A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J.L. & TECH. 4, ¶ 14 (2002), *at* http://www.law.richmond.edu/jolt/v9i1/article4.html.

141. *Id.* ¶ 11.

142. Gregory Hagen, *Sovereign Domains and Property Claims*, 11 INT'L J.L. & INFO. TECH. 1, 4 (2003).

top level domain (TLD).[143] Thus, for the hypothetical domain name, "imaginarydomainname.com," the second level domain would be "imaginarydomainname" and the TLD would be ".com." There are two main types of TLDs: (1) the generic TLD (gTLD), such as .com, .org, and .edu; and (2) the country code TLD (ccTLD), such as .kr (Korea), .uk (United Kingdom), and .ch (Switzerland).[144] While both types of TLDs work in much the same way technically, the rules and policies for registering domain names in the gTLDs and ccTLDs can vary significantly because of how the DNS developed early in its history.[145]

The DNS began in the mid-1980s[146] when the Internet Assigned Numbers Authority (IANA), a group of scientists funded by the U.S. Department of Defense, implemented and managed the DNS until 1992.[147] During this period, IANA delegated registration of ccTLDs to country managers[148] who operate them according to local policies that are adopted to best meet the economic, cultural, and linguistic circumstances of the country or territory involved.[149] When IANA delegated ccTLD registration to country managers, it did so without entering into formal written agreements.[150] In 1992, the National Science Foundation, a U.S. administrative agency, took over the civilian fund-

143. *See* BENDER, *supra* note 11, § 3D.05(1).

144. von Arx & Hagen, *supra* note 140, ¶ 12. There is also a third type of TLD, the iTLD, which is used solely for infrastructure purposes and does not affect the normal user in any way. *Id*.

145. ICANN, *The Internet Domain Name System and the Governmental Advisory Committee (GAC) of ICANN* (2001), *at* http://www.icann.org/committees/gac/outreach-en-01oct01.htm.

146. ICANN, *March 2000 ICANN Meeting in Cairo: ccTLD Delegation and Administration Policies* (2000), *at* http://www.icann.org/cairo2000/cctld-topic.htm.

147. Weinberg, *supra* note 136, at 198.

148. "TLD managers are trustees for the delegated domain, and have a duty to serve the community. The designated manager is the trustee of the TLD for both the nation, in the case of ccTLDs, and the global Internet community." ICANN, *ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)*, *at* http://www.icann.org/icp/icp-1.htm.

149. ICANN, *March 2000 ICANN Meeting in Cairo: ccTLD Delegation and Administration Policies* (2000), *at* http://www.icann.org/cairo2000/cctld-topic.htm.

150. von Arx & Hagen, *supra* note 140, ¶ 32.

ing of the DNS and contracted with Network Solutions, Inc. (NSI) to manage the DNS,[151] which lasted until 1998.[152]

Today, management of the DNS is in a transitional phase from the U.S. government to the Internet Corporation for Assigned Names and Numbers (ICANN).[153] This transition began in 1998 with the creation of ICANN through a Memorandum of Understanding between the U.S. Department of Commerce and ICANN.[154] Under the latest Memorandum of Understanding, to complete the transition of the DNS management, ICANN must enter into agreements with all of the existing managers of the ccTLDs as well as the governments of the affected countries or territories, which IANA had not done when it initially delegated the ccTLDs to country managers.[155] Since 2000, ICANN has been pressuring ccTLD managers to enter into formal contractual relationships.[156] However, to date, only twelve out of the 246 ccTLDs have entered into such contracts.[157] The remainder

151. BENDER, *supra* note 11, § 3D.05(2).

152. NSI's control over the DNS proved to be an inequitable situation. *Development: V. The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1663 (1999). With NSI's monopoly over the registration of new domain names, potential registrants had no alternatives to NSI, which some registrants claimed had poor customer service, and other entities were prevented from becoming registrars in the lucrative domain name business. *Id*. Furthermore, NSI's procedure for domain name registration led to the problem of cybersquatting because NSI asserted that the registration of a domain name did not establish a trademark right to that domain name. *Id*. Under NSI's registration procedure, NSI registered domain names on a first-come, first-served basis and made it the registrant's responsibility to ensure that the domain name it registered did not infringe upon any trademark rights. *Id*. Because of NSI's policy to register domain names on a first-come, first-served basis, "cybersquatters" were able to register domain names of value in order to resell them for profit to the business normally associated with that name or to publicly criticize the owner or product of the trademark. *Id*.

153. ICANN, *Fact Sheet*, *at* http://www.icann.org/general/fact-sheet.html. ICANN is "a public benefit, non-profit entity" and is responsible for the management and oversight of the coordination of the DNS. *Id*.

154. *See* BENDER, *supra* note 11, § 3D.05(2).

155. ICANN, *March 2000 ICANN Meeting in Cairo: ccTLD Delegation and Administration Policies* (2000), *at* http://www.icann.org/cairo2000/cctld-topic.htm.

156. von Arx & Hagen, *supra* note 140, ¶ 32.

157. To date, only Australia (.au), Kenya (.ke), Japan (.jp), Sudan (.sd), Taiwan (.tw), Uzbekistan (.uz), Palestine (.ps), Nigeria (.ng), Afghanistan (.af), Burundi (.bi), Laos (.la), and Malawi (.mw) have entered into ccTLD agree-

of the ccTLDs, including Switzerland's ".ch" ccTLD, which Otamedia's website now operates under, are each still operated by the country managers, independent of ICANN.[158] Thus, the DNS is not governed by a single entity; ICANN manages the gTLDs and only twelve ccTLDs,[159] while 234 ccTLDs are managed independently by country managers.[160]

Turning back to Philip Morris's suit against Otamedia, Otamedia registered its ".com" domain names with NSI,[161] the same Virginia-based company that managed the DNS from 1992 to 1998.[162] When Philip Morris sought to obtain ownership of these domain names, NSI informed both parties that "the disputed domain name registration will not be transferred, suspended, or otherwise modified during the pendency of th[is] action, except upon order of the court."[163] Because NSI is an American corporation, the District Court unquestionably had the power to order NSI to transfer Otamedia's domain names to Philip Morris. On the other hand, Otamedia registered its Swiss ".ch" domain names with SWITCH: The Swiss Education and Research Network, the country manager for the ".ch" and ".il" ccTLDs.[164] Under SWITCH's General Terms and Conditions, SWITCH will transfer a domain name to a third party on the basis of a decision or settlement, if it is presented with a court or arbitration decision enforceable in Switzerland and a certificate on the enforceability of the decision.[165] Thus, for

---

ments with ICANN. *See* ICANN, *ccTLD Agreements*, *at* http://www.icann.org/cctlds/agreements.html. For a list of all the existing ccTLDs, *see* IANA, *Root-Zone Whois Information: Index by TLD Code*, *at* http://www.iana.org/cctld/cctld-whois.htm.

158. Hagen, *supra* note 142, at 5.

159. *See* ICANN, *ICANN Information*, *at* http://www.icann.org/general/ (last visited May 23, 2005).

160. *See* ICANN, *ccTLD Agreements*, *at* http://www.icann.org/cctlds/agreements.html (last visited May 23, 2005).

161. *Philip Morris*, 331 F. Supp. 2d at 230.

162. *See* ICANN, *Fact Sheet*, *at* http://www.icann.org/general/fact-sheet.html (last visited May 23, 2005).

163. *Philip Morris*, 331 F. Supp. 2d at 230.

164. *See* SWITCH website, *at* http://www.switch.ch/about/activities.html ("Since the introduction of the Internet in Switzerland, SWITCH has been registering domain names ending in .ch and .li.").

165. SWITCH, *General Terms and Conditions (GTC) for the registration and administration of domain names below the domain ".ch" and ".il,"* ¶ 3.4.2, *at* http://www.switch.ch/id/terms/agb_v6_print.html.

Philip Morris to obtain Otamedia's Swiss-registered domain names, it would have to present SWITCH with a court or arbitration decision enforceable in Switzerland.

However, in the event that the District Court does modify its order to include Otamedia's Swiss domain names,[166] Philip Morris might not succeed in enforcing such an order in Switzerland because, as a general rule, trademark rights do not extend beyond the territory of a nation.[167] U.S. trademark owners cannot enforce their trademark rights in other countries because of the territoriality principle.[168] Therefore, "[t]he concept of global economy does not automatically translate to global trademark protection. Each country has its own trademark laws, procedures, and enforcement schemes."[169] In order for Philip Morris to obtain Otamedia's Swiss domain names, it would have to sue Otamedia in Switzerland under Swiss trademark law[170] or seek extraterritorial application of a U.S. court order[171] that a Swiss court deems enforceable under Swiss law.

Thus, the litigation between Philip Morris and Otamedia exemplifies the impracticality of seeking domain names registered

166. The Southern District of New York denied Philip Morris's request to order the transfer of Otamedia's Swiss domain names *without prejudice*, leaving open the possibility that the court will order the transfer of the Swiss domain names later. *Philip Morris*, 331 F. Supp. 2d at 231 n.3.

167. Bella I. Safro & Thomas S. Keaty, *What's in a Name? Protection of Well-Known Trademarks Under International and National Law*, 6 TUL. J. TECH. & INTELL. PROP. 33, 34 (2004). *See also* Paris Convention for the Protection of Industrial Properties, July 14, 1967, art. 6(3), 21 U.S.T. 1583 ("A mark duly registered in a country of the Union shall be regarded as independent of marks registered in the other countries of the Union, including the country of origin.").

168. Safro & Keaty, *supra* note 167, at 34.

169. *Id*.

170. Federal Act 232.11, *translated in* http://www.swisstm.ch/tradeact.html.

171. Whether the District Court can apply the Lanham Act extraterritorially to reach Otamedia's Swiss domain names rests on three factors: "(1) whether the defendant's conduct has a substantial effect on United States Commerce; (2) whether the defendant is a citizen of the United States; and (3) whether there exists a conflict between defendant's trademark rights established under foreign law, and plaintiff's trademark rights established under domestic law." Sterling Drug, Inc. v. Bayer AG, 14 F.3d 733, 745 (2d Cir. 1994). Under international law, a state has jurisdiction to apply its laws extraterritorially with respect to conduct that has or is intended to have substantial effect within its territory. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1)(c) (1987).

abroad as a remedy against offshore websites. Although Philip Morris certainly has the financial means to sue Otamedia in Switzerland, "American trademark owners and attorneys are most likely not familiar with the court system in foreign nations. Litigation in a foreign country can be very costly and, despite the added expense, the result is often uncertain."[172] The geographical safe haven under the current structure of the DNS is compounded by the fact that offshore websites can also find virtual safe havens by providing their domain name registrar with false names and contact information.[173] Thus, trademark owners could have difficulty ascertaining the true identity of such registrants.[174] In addition, not all ccTLD registrars require the domain name registrant to operate its website from within that country's territory.[175] Thus, an offshore website could operate from country *X*, but register its domain names in countries *Y* and *Z* in an effort to hide its location and identity, and ultimately avoid any enforcement measures taken against it.

Indeed, Otamedia sought both geographical and virtual safe havens in its online cigarette operation.[176] Otamedia first incorporated in the Isle of Man, then in Belize, while conducting its business in Switzerland.[177] Also, Otamedia tried to hide its corporate identity by registering domain names under different entities.[178] For instance, Otamedia registered its Swiss domain names yesmoke.ch and yessmoke.ch under the entity "Yesmoke Tobacco, S.A.," and registered yespeedy.ch, yesspeedy.ch, and yes-speedy.ch under the entity "Yespeedy Ltd."[179] All of these

172. Xuan-Thao N. Nguyen, *The Digital Trademark Right: A Troubling New Extraterritorial Reach of United States Law*, 81 N.C. L. REV. 483, 491 (2003).

173. *Id*. at 506.

174. *Id*.

175. For example, SWITCH does not require registrants to operate their websites from Switzerland. *See* SWITCH, *supra* note 165, ¶ 2. Also, "[w]ith an attractive country code TLD, such as the South Pacific nation of Tuvalu and its '.tv,' governments are profiting handsomely…by opening their domains to a global audience, marketing themselves as an alternative to the increasingly crowded '.com' namespace." Navin Katyal, *The Domain Name Registration .bizness: Are we being "Pulled Over" on the Information Super Highway?*, 24 HASTINGS COMM. & ENT. L.J. 241, 259 (2002).

176. *See Philip Morris*, 331 F. Supp. 2d at 229 n.1.

177. *Id*.

178. *See id*.

179. SWITCH, *Domain Name Search*, *at* http://www.switch.ch/id/search-domain.html?mode=basic (last visited May 23, 2005).

domain names led to the same Otamedia website Philip Morris has been attempting to enjoin.[180] Furthermore, Otamedia is not the only cigarette website operator that has taken advantage of the virtual safe haven within the current DNS.[181] In early 2004, a U.S. District Court in Los Angeles transferred to Philip Morris the domain name of the cigarette website allsmoke.com.[182] In response, the website relocated to a Russian web server and continued to sell Philip Morris brands at its new Russian-registered domain name, allsmoke.ru.[183]

Thus, Otamedia and allsmoke.ru provide examples of how "given the strict territorial limits on enforcement, small actors who are deliberate in maintaining no assets or contacts with a forum will continue to be a problem."[184] Furthermore, because extraterritorial enforcement of a judgment will always be subject to some form of scrutiny by foreign courts, offshore websites can easily remove their assets to a safe harbor in any jurisdiction which will refuse to recognize that judgment.[185] In the context of Philip Morris's trademark infringement suits against offshore cigarette websites, "[i]n the absence of enforcement, intellectual property laws could easily be circumvented by the creation of Internet sites that permit the very distribution that has been enjoined [by a U.S. court]."[186] Given these difficulties in enforcing judgments against offshore websites, the solution may lie in the use of filtering technology domestically. The next

180. These domain names were last visited on December 22, 2004.

181. *See* Dunai, *Duty-Free*, *supra* note 37, at B1.

182. *Id*.

183. *Id*. After registering its Russian domain name, Allsmoke posted on its website, "we have opened an additional domain name not to depend on decision of American courts [sic]. American courts [sic] decisions can not be applied to any national domains extensions [sic]. Domain name Allsmoke.ru refers to Russian legislation and that is why American laws can not be applied in this case." Allsmoke, *We Have Changed Our Address to Allsmoke.ru*, Mar. 19, 2004, *at* http://www.allsmoke.ru/allnews.html#ru (last visited Dec. 23, 2004). However, on October 26, 2004, Allsmoke posted on its website, "Dear clients! We inform [sic] that we resume shipping of orders excluding United States. Shipping to the United States will be available soon." Allsmoke, *at* http://www.allsmoke.ru/allnews.html#ru (last visited Dec. 23, 2004).

184. Fagin, *supra* note 3, at 451.

185. Horatia Muir Watt, *Yahoo! Cyber-Collision of Cultures: Who Regulates?*, 24 MICH. J. INT'L L. 673, 690 (2003).

186. Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032, 1040 (S.D.N.Y. 1996).

part of this Note will explore two instances of government-mandated uses of filtering technology.

III. GOVERNMENT-MANDATED FILTERING

In May 2000, a French court ordered Yahoo! "to take all measures at its availability to dissuade and render impossible all visitation on Yahoo.com [by French users] to participate in the auction service of Nazi paraphernalia, as well as to render impossible any other site or service which makes apologies of Nazism or that contests Nazi crimes."[187] The court found that Yahoo! is capable of identifying the geographical origin of users who visit its site, which therefore should provide Yahoo! with the means to prohibit users in France from accessing the site. In response to Yahoo!'s subsequent assertion that compliance with the order is technologically impossible, the court established an expert panel to study the feasibility of filtering out French users from the Yahoo! auction site.[188]

In November 2000, based on the expert panel's reports, the French court found that seventy percent of the IP addresses of French users could be correctly identified and blocked from accessing Yahoo! pages displaying Nazi material (geo-location filtering).[189] However, the court also found that users can hide their geographical location by using "anonymizer sites,"[190] which can replace the user's real IP address with another address, thereby making the geographical location of the user unknown.[191] For users whose location cannot be determined, the expert panel suggested that Yahoo! could request users to declare their nationality at the Yahoo! auction page or before

187. UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, May 22, 2000, obs. C. Bensoam & J. Gomez, *translated in* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm [hereinafter Yahoo *I*].

188. Marc H. Greenberg, *A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market*, 18 BERKELEY TECH. L.J. 1191, 1210 (2003).

189. Yahoo *II*, T.G.I. Paris, Nov. 22, 2000.

190. Anonymizer sites use "anonymous proxy servers" which can keep an internet user's identity secret. When visiting a website through an anonymizer site, the request to visit the website appears to the ISP as a request directed to the anonymizer site rather than the underlying website to which the user actually seeks access. Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606, 643 (E.D. Pa. 2004).

191. Yahoo *II*, T.G.I. Paris, Nov. 22, 2000.

searching for Nazi objects.[192] With the combination of geo-location filtering and the declaration of nationality by users seeking to access the site, the court found that Yahoo! could achieve ninety percent compliance.[193] Based on these findings, the court ordered Yahoo! to comply with its May 2000 order to filter out French users from the auction site.[194]

Yahoo!, however, ultimately never implemented the geo-location filtering ordered by the French court.[195] In December 2000, Yahoo! sued UEJF and LICRA in the United States District Court for the Northern District of California for a declaratory judgment that the French court's order is unenforceable in the United States on the grounds that the order violates the First Amendment.[196] However, before the District Court ruled on the merits, Yahoo! removed the Nazi memorabilia from its auction site.[197] Despite the removal of the Nazi memorabilia, the District Court ruled that the French order violated Yahoo!'s First Amendment rights and was therefore unenforceable in the United States.[198]

Because Yahoo! never complied with the French court's order, the accuracy of the experts' estimates cannot be determined. However, geo-location filtering has since been criticized as being ineffectual.[199] First, it is only eighty to ninety-nine percent accurate and, second, it is easily circumscribed.[200] One of the experts impaneled to report to the French court later criticized

192. *Id*.

193. *Id*.

194. *Id*.

195. *See* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 276 (2002).

196. *See* Greenberg, *supra* note 188, at 1210.

197. *See* Reidenberg, *supra* note 195, at 276.

198. *See* Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001). Also, in February 2003, a French criminal court dismissed charges against the former Yahoo! CEO for condoning war crimes by selling Nazi memorabilia. Lawrence W. Newman & David Zaslowsky, *Jurisdiction Through the Internet*, N.Y. L.J., Feb. 26, 2003, at 3 n.2.

199. *See* Greenberg, *supra* note 188, at 1215.

200. *See id*; *see also* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 811 (2001) (Geo-location filtering "correctly identifies the content receivers' geographical identity at the national level between ninety and ninety-eight percent of the time, but at the state level only eighty to ninety-five percent of the time.").

the court's order as "half-assed and trivially avoidable" because the order can easily be circumvented by using an anonymizer site or by lying when the site prompts the user to give a declaration of nationality.[201] Furthermore, geo-location filtering raises "concerns about the preservation of the privacy rights of surfers to be free of software that identifies them as they surf the net."[202]

On the other hand, "[i]n contrast to the enforcement problems created by the Internet's locational ambiguity, geographic identification empowers states to implement a variety of public policies within their territories, including the enforcement of intellectual property rights, consumer protection, and data privacy through geographic filtering."[203] The use of filtering technology as an enforcement tool in the *Yahoo!* case shows that internet sites can be made inaccessible from within a country's borders.[204] Thus, filtering technology "readily bypasses … all the familiar difficulties generally linked to international enforcement of legislative prescriptions or judicial decisions in the real world."[205] Filtering technology could free courts from the need to rely on the ineffectual enforcement techniques of the physical world against offshore websites.[206] If a court employs filtering technology to block access to offshore websites that violate domestic law, such website operators can no longer ignore the risk of liability or criminal sanctions in the hope that traditional enforcement means cannot reach it.[207]

Rather than mandating geo-location filtering on offshore website operators as the French court did against the unwilling Yahoo!, nations themselves should use filtering to block their own citizens from accessing illegal material on the internet.[208] Ordering an offshore website to implement filtering may be ineffective because an offshore website may simply ignore a foreign court order, as Otamedia has done, or seek judicial invali-

201. Ben Laurie, *An Expert's Apology*, *at* http://www.apache-ssl.org/apology.html (last visited May 23, 2005).
202. Greenberg, *supra* note 188, at 1215.
203. Reidenberg, *supra* note 195, at 278.
204. *See* Muir Watt, *supra* note 185, at 679.
205. *Id*.
206. *See id*. at 690.
207. *See id*. at 691.
208. *See* Fagin, *supra* note 3, at 451.

dation of the foreign court order in the offshore website's home state, as Yahoo! has done.[209] On the other hand, governmental use of filtering technology would avoid exertion of extraterritorial jurisdiction over offshore websites and minimize impact on the internet's infrastructure because filtering does not control the actual content on the internet, it merely controls what content users can access.[210] Nations should utilize filtering technology at the level of their domestic ISPs to enforce judgments against offshore websites because such technology "is less restrictive and intrusive than uncertain and inefficient judicially crafted case-specific remedies."[211] Thus, government-mandated use of filtering technology by ISPs may present a viable solution to preventing U.S. consumers from purchasing cigarettes from offshore websites like Otamedia that thus far have evaded "uncertain and inefficient judicially crafted case-specific remedies."

Pennsylvania attempted the kind of government-mandated filtering by ISPs proposed above, but the Eastern District of Pennsylvania struck it down as unconstitutional.[212] The use of government-mandated filtering by ISPs in Pennsylvania began in February 2002, when Pennsylvania enacted the Internet Child Pornography Act (the Act),[213] which requires ISPs to remove or disable access to child pornography residing in or accessible through their service upon notification by the Pennsylvania Attorney General.[214] To implement the Act, the Office of the Attorney General established the Child Sexual Exploitation Unit (CSEU) which would issue an informal notice to an ISP of

209. *See id*. at 419 ("'[O]ffshore actors are unlikely to implement geolocation technologies voluntarily, and, without influence of indirect state action, will remain beyond the effective reach of states.").

210. *Id*. at 451–52.

211. *Id*. at 403.

212. *Center for Democracy & Technology*, 337 F. Supp. 2d at 655.

213. 18 Pa. Cons.Stat. §§ 7621–30 (2004).

214. Under the Act:

> An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.

Duty of Service Provider, 18 Pa. Cons.Stat. § 7622 (2004).

child pornography residing in or accessible through its service and the ISP would be required to remove the items or disable access.[215] The informal notices identified the uniform resource locator (URL)[216] of the child pornography site(s).[217] The CSEU enforced the Act from April 2002 to September 2003, when the Center for Democracy & Technology,[218] the ACLU, and Plantagenet[219] filed a complaint for declaratory and injunctive relief, claiming that the informal notices and the Act violate the First Amendment and the Dormant Commerce Clause.[220]

At trial, several Pennsylvania ISPs[221] testified as to the feasibility of three types of filtering: DNS[222] filtering, IP[223] filtering, and URL filtering.[224] DNS filtering involves an ISP making entries in the DNS servers under its control that prevent requests to those servers for a specific website's domain name from converting to its corresponding IP address.[225] Implementation of DNS filtering would not require ISPs to purchase new equipment, and if the ISP's staff is familiar with DNS filtering, implementation would be inexpensive and require little staff time.[226] However, DNS filtering is more difficult to implement than IP filtering because it is a more specialized technique, not

---

215. *Center for Democracy & Technology*, 337 F. Supp. 2d at 620–21. The Office of the Attorney General and the ISPs in Pennsylvania agreed to follow an informal notification procedure rather than the formal statutory procedure set forth in § 7628 of the Act, which required a court order and criminal sanctions for noncompliance, because the ISPs were concerned that in some instances compliance may be technically impossible. *Id*. at 621.

216. "A URL is the commonly used textual designation of an Internet web site's address." *Id*. at 615.

217. *Id*. at 623.

218. The Center for Democracy & Technology is a nonprofit corporation devoted to internet issues. *See id*. at 612.

219. Plantagenet, Inc. is an ISP incorporated in Pennsylvania. *See id*.

220. *Id*. at 611–12.

221. The following ISPs testified at trial: America Online, Comcast IP Services, Epix Internet Services, Pennsylvania Online, Verizon Internet Services, and Worldcom. *See id*. at 627–28.

222. "DNS" stands for Domain Name System. *See supra* Part II.

223. "IP address" stands for Internet Protocol address, a unique identifying number for each computer comprising a part of the internet which consists of four groups of digits separated by a period. *See supra* Part II.

224. *See Center for Democracy & Technology*, 337 F. Supp. 2d at 627–28.

225. *Id*.

226. *Id*. at 629.

a standard process, and not something that ISPs normally do.[227] The ISPs America Online and Worldcom, which do not utilize DNS filtering, both testified that implementing DNS filtering to their networks would be difficult.[228] Furthermore, DNS filtering would not be effective for customers who do not use the DNS servers provided by their ISP, such as the many large businesses that operate their own DNS servers.[229] Also, DNS filtering can lead to significant overblocking of innocent websites because it blocks requests for all subpages under the blocked domain name and those subpages may contain innocent content.[230]

IP filtering involves an ISP determining the IP address of a specific URL; the ISP then makes entries in its routing equipment that will block requests for the specific IP address.[231] Most ISPs already have the hardware needed to implement IP filtering, and ISPs routinely use IP filtering to respond to attacks on their networks.[232] Most ISPs can implement IP filtering without having to purchase additional equipment, and many ISPs already have an existing internal procedure to implement IP filtering.[233] Unlike DNS filtering, IP filtering would be effective even when a user does not rely on the ISP's DNS server.[234] However, a website can evade IP filtering by obtaining a new IP address for its website without changing its URL, but an ISP can counteract this practice by monitoring the website for changes to its IP address.[235] Like DNS filtering, IP filtering re-

227. *Id*.

228. *Id*. For America Online, "automating this process would involve designing a new system to do DNS filtering, assessing the related risks, assigning additional long-term staff, and developing auditing and monitoring systems." *Id*. For Worldcom, "implementing DNS filtering would require [it] to purchase and configure additional DNS servers in its network and potentially reconfigure the systems of millions of customers." *Id*. at 630.

229. *Id*. at 631.

230. *See id*. at 633. For example, if DNS filtering blocked the hypothetical domain name "x.com" because its subpage, "x.com/subpage," contains child pornography, then all the other subpages of the domain name, which contain only innocent content, would also be blocked.

231. *Id*. at 628.

232. *Id*. at 629.

233. *Id*.

234. *Id*. at 632.

235. *Id*. Worldcom uses this technique of IP address monitoring, thus preventing websites from evading a block placed on its site by Worldcom. *Id*.

sults in a significant amount of overblocking because many websites can share a single IP address.[236]

URL filtering involves the placement of an additional device, or in some cases the reconfiguration of an existing router or other device, in an ISP's network that reassembles the internet traffic flowing through its network, reads each user's requested URL, and if the requested URL matches one of the URLs specified in a blocking order, discards or blocks the request.[237] No ISPs in Pennsylvania utilize URL filtering.[238] To implement URL filtering, the ISPs testified that they would be required to develop and test new equipment.[239] However, URL filtering presents the most effective method of filtering because, unlike DNS or IP filtering, URL filtering blocks out URLs down to the specific subpage.[240] Thus, URL filtering results in the least amount of overblocking of innocent pages compared to DNS or IP filtering because URL filtering targets only a specific URL of a domain name's subpage and not the entire IP address or domain name.[241] Although the court found URL filtering the most effec-

---

Furthermore, changing the IP address of a website would not evade DNS filtering. *Id*.

236. *Id*. at 633. For example, the court found that the IP address 204.251.10.203 hosted at least 15,575 websites. *Id*. at 638. Thus, if only one of these 15,575 websites contained child pornography, then use of IP filtering would also block the 15,574 *innocent* websites.

237. *Id*. at 628.

238. *Id*. at 630.

239. *Id*. The ISPs testified that URL filtering would require ISPs to purchase switches and routers to maintain the network's prior level of capacity because the switches and routers can handle less traffic if they are performing URL filtering. Unless an ISP purchased more switches and routers, URL filtering would slow down the performance of an ISP's network. *Id*. at 360–61.

240. *Id*. at 634.

241. *Id*. To illustrate, suppose the hypothetical IP address "111.111. 111.111" hosts 500 domain names. Of those 500 domain names, only the hypothetical "xx.com" domain name contains child pornography. Suppose further that "xx.com" contains 100 subpages of which only one subpage contains child pornography. IP filtering would block all 500 domain names, including the 499 innocent domain names. DNS filtering would not block out the 499 innocent domain names, but would block out all 100 subpages of "xx.com," including the 99 subpages that contain only innocent content. However, URL filtering would block out only the single offending subpage, allowing users to access the other 99 innocent subpages of that particular domain name as well as the other 499 innocent domain names within the single IP address.

tive method,[242] it also found that all three methods of filtering could be circumvented through the use of anonymous proxy servers.[243] Despite the effectiveness of URL filtering, because of the additional cost to implement it, the Pennsylvania ISPs used only DNS or IP filtering, rather than URL filtering, to comply with the statute.[244] Therefore, the court did not find URL filtering a feasible alternative to DNS or IP filtering.[245]

The Eastern District of Pennsylvania ultimately held that enforcement of the Act violated the First Amendment because the overblocking of innocent speech through IP and DNS filtering[246] burdened protected speech without alleviating the harms addressed by the Act, namely child pornography, in a direct and material way.[247] Although URL filtering would avoid overblocking, the court noted that the Act does not specify a required method of compliance.[248] The court further found that the Act and the informal notice procedure constitute an unconstitutional prior restraint on speech.[249] The First Amendment requires that a court make a final determination after an adversary hearing that the challenged content is not protected speech before removing such content from circulation.[250] Therefore, the Act violates the First Amendment because it permits a judge to make that determination *ex parte*.[251] The court also held that

242. *Id*.

243. *Id*. at 643. Anonymous proxy servers hide the identity of the internet user and make it appear to the ISP routing the request as if the request is directed at the proxy server rather than the underlying URL to which the user actually seeks access. *Id*.

244. *Id*. at 630.

245. *Id*. at 652.

246. The court found that IP and DNS filtering by the Pennsylvania ISPs resulted in blocking more than 1,190,000 innocent websites in order to block less than 400 child pornography websites. *Id*. at 655.

247. *Id*. at 655–56.

248. *Id.* at 656.

249. "The term 'prior restraint' describes orders forbidding certain communications that are issued before the communications occur." *Id*.

250. *See* Freedman v. Maryland, 380 U.S. 51, 58 (1965).

251. *Center for Democracy & Technology*, 337 F. Supp. 2d at 657. Removing material from circulation constitutes a prior restraint on speech, unless there is a judicial determination in an adversary proceeding that the material contains speech unprotected by the First Amendment. *Freedman*, 380 U.S. at 58. Thus, in addition to the *ex parte* judicial determinations made under the Act, the informal notices issued to ISPs under the Act also constitute prior re-

the Act violates the Dormant Commerce Clause[252] because the burden on interstate commerce imposed by overblocking innocent sites exceeds the local benefit of reducing sexual abuse of children.[253]

IV. A PROPOSED SOLUTION

Because of its effectiveness, URL filtering may provide a solution to enjoining foreign website operators like Otamedia from finding virtual safe havens to reach U.S. consumers. Although the *Center for Democracy & Technology* court found that URL filtering could be circumvented by using anonymous proxy servers, such filtering need not be perfect, but rather need only be reasonably effective to achieve its desired impact.[254] Furthermore, in the context of using URL filtering to block websites like Otamedia that specifically target U.S. consumers, it would be impracticable to operate an online business that has become subject to URL filtering in the hopes that customers are computer-savvy enough to circumvent URL filtering. It would also be impracticable for cigarette websites to periodically change

straints because child pornography is removed from a website pursuant to the informal notice issued by law enforcement rather than a final determination by a judge after an adversary proceeding. *See Center for Democracy & Technology*, 337 F. Supp. 2d at 660.

252. Generally, "[t]he dormant Commerce Clause is a judge-made doctrine that prohibits states from regulating in ways that unduly burden interstate commerce." Goldsmith & Sykes, *supra* note 200, at 786.

253. *Center for Democracy & Technology*, 337 F. Supp. 2d at 662. The court reached this holding by applying the *Pike* balancing test for determining whether a statute that does not facially discriminate against interstate commerce violates the Dormant Commerce Clause. Under the *Pike* balancing test, a state regulation violates the Dormant Commerce Clause if its burden on interstate commerce clearly outweighs its local benefits. *See* Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970). Using URL filtering *nationwide* to block foreign cigarette websites that infringe trademarks, evade taxes, or sell to minors would not raise Dormant Commerce Clause concerns because the Dormant Commerce Clause only applies to state law. *See* Goldsmith & Sykes, *supra* note 200, at 786.

254. *See* Goldsmith & Sykes, *supra* note 200, at 812 ("Regulatory slippage is a fact of life in real space and cyberspace. . . [One should not] assume that imperfections in Internet identification and filtering technology render these technologies useless.").

their domain names to circumvent filtering since potential customers would have difficulty finding such sites.[255]

A federal regulatory system could be developed in which domestic ISPs would be required to use filtering technology to block U.S. internet users from accessing offshore websites that violate U.S. law.[256] By blocking U.S. users from accessing such sites, U.S. court orders would not have to be enforced extraterritorially[257] and offshore websites would be able to conduct activity that is legal in their own country but illegal in the United States.[258] Thus, if the French court in *Yahoo!* had mandated the French ISPs to filter out Yahoo!'s Nazi memorabilia auction site, then Yahoo! could freely exercise its First Amendment rights in the United States while French users would be denied access to the same material, illegal in France.[259]

Government-mandated filtering should be limited to court orders to block a particular website from U.S. access rather than law enforcement officials unilaterally deciding which sites to block. In this way, a defendant-website would be given notice and an opportunity to be heard before a judicial determination

255. *Cf.* Russell B. Weekes, Note, *Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet?*, 8 VA. J.L. & TECH. 4, *65 (2003) (arguing that relying on predetermined lists of IP addresses and domain names to filter out inappropriate content is problematic because "new sites are constantly coming online and content on old sites change frequently.").

256. Preventing internet users from accessing websites that conduct activity that is illegal in their own country allows countries to protect their values in their own territories. *See* Reidenberg, *supra* note 195, at 276.

257. Avoiding extraterritorial enforcement of U.S. law is consistent with "[t]he disfavored status within international law of unilateral state-based regulations that target extraterritorial actors [that] arises from the inherent challenges such actions represent to state sovereignty." Fagin, *supra* note 3, at 396.

258. Creating a site that complies with the local laws of all nations "may prove . . . daunting and would doubtless reduce Internet sites to a level of blandness that would eventually sap all interest in the Internet as an effective means of communication between nations." Greenberg, *supra* note 188, at 1215. Thus, by requiring ISPs to filter sites that violate U.S. law so that only U.S. users are denied access, "[c]ourts can limit the restrictive effect of regulation and incriminations to activities that directly affect welfare within their own jurisdiction. Unnecessary regulatory spillover can be avoided if restrictions to the free flow of information, for example, can be limited to a given set of geographically located users." Muir Watt, *supra* note 185, at 689.

259. *See supra* Part III.

that the website should be filtered from U.S. access.[260] The use of government-mandated filtering should further be limited to enforcing judgments when traditional remedies prove ineffective.[261] For example, if Philip Morris wants to enjoin website operators like Otamedia from selling its brands without authorization and from infringing federal trademark law, it should continue litigating against them and seek a traditional prohibitory injunction.[262] In the event that the defendant-website refuses to comply with the injunction, Philip Morris could seek to modify the injunction by entry of a court order for domestic ISPs to filter the website from U.S. access.[263] By narrowly limiting the use of government-mandated filtering, courts

260. This adversary hearing requirement is proposed because it would only be fair that defendant-websites have an opportunity to be heard before their website is denied the entire American audience. In addition, the adversary hearing requirement ensures that any government-mandated filtering does not block constitutionally protected speech. The Supreme Court held that "because only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint [on speech]." Freedman, 380 U.S. at 58. Without such procedural safeguards, government-mandated filtering may be a prior restraint on speech in violation of the First Amendment. *See id*. at 60.

261. "The historic injunctive process was designed to deter, not to punish." Hecht Co. v. Bowles, 321 U.S. 321, 329 (1944). Therefore, defendant-websites that lose on the merits should be given the opportunity to comply with an injunction ordering the website to cease its illegal activity and only when the website refuses to comply should the more extreme remedy of filtering the site from U.S. access be accorded.

262. A "prohibitory injunction" is a court order that forbids or restrains an act. BLACK'S LAW DICTIONARY 349 (2d Pocket ed. 2001).

263. The Supreme Court has stated:

> A sound judicial discretion may call for the modification of the terms of an injunctive decree if the circumstances, whether of law or fact, obtaining at the time of its issuance have changed, or new ones have since arisen. The source of the power to modify is of course the fact that an injunction often requires continuing supervision by the issuing court and always a continuing willingness to apply its powers and processes on behalf of the party who obtained that equitable relief.

Sys. Fed'n No. 91 v. Wright, 364 U.S. 642, 647 (1961). Therefore, if a defendant-website refuses to comply with a prohibitory injunction, those circumstances may warrant the modification of the injunction to include filtering the website from U.S. access.

can avoid unduly burdening the free flow of information over the internet and resistance from the regulated ISPs.[264]

In addition, government-mandated filtering should be on a nationwide level and only used to enforce federal law to avoid conflicting state laws or Dormant Commerce Clause concerns.[265] Congress could establish an administrative agency under its Commerce Clause power to regulate ISPs that operate within the United States.[266] Under this proposed administrative agency, all ISPs operating within the United States would be required to obtain a license; for ISPs that do not already use URL filtering or some other effective filtering method that does not result in overblocking, implementation of such filtering technology would be a requirement to obtain a license.[267] In this

264. *See* Muir Watt, *supra* note 185, at 693.

265. Some courts have invalidated state statutes that regulate the internet on Dormant Commerce Clause grounds. *See* Goldsmith & Sykes, *supra* note 200, at 790–95. Also, filtering on a nationwide level would be much easier for ISPs than filtering websites for a particular state. *See Center for Democracy & Technology*, 337 F. Supp. 2d at 620 (noting that the Pennsylvania ISPs complained that blocking access to a website for Pennsylvania users only would be technically impossible, but blocking access nationwide would not be).

266. U.S Const. art. I, § 8 ("Congress shall have the power . . . [t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."). Under Congress's Commerce Clause power, Congress may regulate the channels and instrumentalities of interstate commerce and activities that have a substantial effect on interstate commerce. United States v. Morrison, 529 U.S. 598, 609 (2000). Therefore, Congress has the power to regulate ISPs under the Commerce Clause because the innumerable business transactions that occur through an ISP's servers make ISPs channels of interstate commerce, or alternatively, have a substantial effect on interstate commerce.

267. On the difficult question of who should pay for the URL filtering technology for ISPs to implement, one commentator argues that "[t]he State in which the effects are suffered obviously has a greater incentive to ensure watertight enforcement of its own restrictive regulation: it would certainly make more sense to leave it to filter the undesired data, to avoid the risk of underenforcement." Muir Watt, *supra* note 185, at 693. On the other hand, "some regulating States with legitimate reasons to filter data may lack the technological means or public resources to do so. . . . As a result, it might appear more equitable to burden private service providers generating revenue from activities directed at the regulating State rather than on the population of the regulating State." *Id*. at 694. Perhaps the federal government could assist the existing U.S. ISPs with the cost of implementation as they transition into this proposed regulatory regime and thereafter require any new companies

way, the proposed agency would have a database of all the ISPs operating within the United States, and all the ISPs would have effective filtering technology in place. Upon a federal court order to filter a website from U.S. access, the proposed agency would notify the ISPs of the order. ISPs would be given a reasonable time period to filter the website. The proposed agency would monitor the ISPs to ensure compliance and conduct administrative hearings to issue civil penalties against ISPs that fail to comply with a court order.[268] In the event that the filtering proves ineffective in that U.S. users can still access the website through a particular ISP, or an ISP's filtering results in overblocking of innocent sites, the ISP would be afforded a reasonable efforts affirmative defense to avoid penalty.[269] The proposed agency would also have the task of periodically monitoring the URLs that have been filtered to check whether the website still violates the law.[270] Periodic monitoring would ensure that URLs with innocent content would not be blocked from U.S. users. In the event that a website changes its content to comply with U.S. law, it can apply to the proposed agency to have a block removed. The proposed agency could then review the contents of the URL to check whether the content changes warrant removal of the block.

---

seeking to enter the ISP market to pay for the filtering technology themselves before obtaining a license.

268. Administrative agencies have legislative power to promulgate regulations, executive power to enforce their rules, and judicial power to adjudicate them. Administrative law judges hear cases brought by agency officials against those accused of violating the agency's regulations. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES § 3.10.1 (2d ed. 2002).

269. *See* Muir Watt, *supra* note 185, at 690 ("[I]t would be fair to provide a 'reasonable efforts' defense to protect service providers who have taken care to comply.").

270. *See* Weekes, *supra* note 255, at *65 (arguing that for reliable efficacy of filtering based on lists of IP addresses and domain names, the lists must be updated constantly because content on sites changes frequently). *Cf. Center for Democracy & Technology*, 337 F. Supp. 2d at 662 (preventing future content from being displayed at a URL based on the fact that the URL contained illegal material in the past would be an unconstitutional prior restraint on speech).

V. CONCLUSION

Over the course of the internet's brief history, it has experienced unimagined growth. Internet users worldwide have enjoyed the benefit of the free flow of information as well as access to a global market with the click of a button. However, as the internet experiences this amazing expansion, national governments justifiably must seek ways to protect their citizens from the ever-increasing harms lurking within this global network. While this Note specifically addressed the harms of online cigarette sales, governments have drawn their attention to the many other dangers now found on the internet.[271] However, because of the anonymity and geographical indeterminacy afforded by the internet's architecture, smaller actors can seek virtual safe havens in bad faith to avoid traditional enforcement techniques and flout foreign judgments against them, just as Otamedia has done with its online cigarette operation.

Philip Morris and the Southern District of New York believed that they found an effective means of reaching such bad faith small actors by seizing the virtual doors of Otamedia's website.[272] However, as evidenced by Otamedia's actions, under the current structure of the DNS, where one door is sealed, many others can be opened. Seeking domain names to enjoin extraterritorial conduct does not serve as an effective remedy because the DNS is in a transitional and decentralized stage, making the enforceability of a foreign judgment ordering the transfer of a domain name uncertain. Furthermore, the remedy of seizing the domain name of an offshore website may not be a fair solution when the conduct of the website is perfectly legal in the country where it is physically located, but happens to be illegal in the country ordering that the domain name be seized.[273]

---

271. *See, e.g.*, United States v. American Library Ass'n, Inc., 539 U.S. 194 (2003) (material harmful to children); United States v. Ansaldi, 372 F.3d 118 (2d Cir. 2004) (date-rape drug); United States v. Nelson, 383 F.3d 1227 (10th Cir. 2004) (illegally sold prescription drugs); United States v. D'Ambrosia, 313 F.3d 987 (7th Cir. 2002) (gambling); United States v. Dockery, 401 F.3d 1261 (11th Cir. 2000) (child pornography); People v. Davis, 353 Ill. App. 3d 790 (Ill. App. Ct. 2004) (identity theft and computer fraud).

272. *See Philip Morris*, 331 F. Supp. 2d at 245.

273. *See, e.g.*, Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

Therefore, this Note's proposed solution of mandating ISPs to filter a website from U.S. access avoids the difficulties of enforcing judgments extraterritorially or enjoining bad faith small actors who find virtual safe havens within the DNS. Such filtering, used in conjunction with traditional enforcement techniques, would ensure compliance with U.S. judgments and make evasion by small actors too costly.[274] However, the filtering cases discussed above teach us that any government-mandated filtering from within the United States must be carefully crafted to avoid unduly burdening protected speech or interstate commerce.[275] Overuse of filtering within the United States would also raise concerns about the overall quality and usefulness of the internet as an informational tool.[276]

Although URL filtering has yet to be widely implemented by ISPs in the United States,[277] filtering technology has developed rapidly. As with any new technology, over time, the effectiveness of filtering technology will increase while its cost will decrease.[278] Although most ISPs may not have the means or the willingness to implement such technology today, they undoubtedly will in the very near future. As a result, national governments will find they have an effective technological means of

274. *See* Goldsmith & Sykes, *supra* note 200, at 812 ("Computer-savvy users might always be able to circumvent identification technology, just as burglars can circumvent alarm systems. But they would do so at a certain cost, and this cost would be prohibitive for most."); *see also* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996) ("A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially.").

275. *See generally* Patrick M. Garry, *The Flip Side of the First Amendment: A Right to Filter*, 2004 MICH. ST. L. REV. 57 (2004) (discussing First Amendment concerns raised by government-mandated internet filtering in public libraries); Goldsmith & Sykes, *supra* note 200, at 790–95 (reviewing cases which invalidate state internet regulations on Dormant Commerce Clause grounds).

276. *See* Greenberg, *supra* note 188, at 1216 (arguing that over-regulation of the internet could result in "dumbed down" versions of websites).

277. *See Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 630 (E.D. Pa. 2004).

278. *See* Goldsmith & Sykes, *supra* note 200, at 812 ("[T]here is good reason to believe that geographical identification technology will be precise and inexpensive in the near future.").

regulating online activity within their own territory without impeding the free flow of information globally.

Michael Kwon[*]

* B.A., Binghamton University, SUNY (2000); J.D., Brooklyn Law School (Expected 2006); Editor-in-Chief (2005–2006). I would like to thank Erin McMurray, Gena Usenheimer and Samantha Ettari for their assistance with editing and invaluable guidance, and Professor Claire R. Kelly of Brooklyn Law School for her sagacious advice.