COURT OF APPEALS OF KENTUCKY
NO. 2008-CA-2036
(Related to 2008-CA-2000 and 2008-CA-2019)

VICSBINGO.COM and INTERACTIVE GAMING COUNCIL — PETITIONERS

v.

HONORABLE THOMAS D. WINGATE and
COMMONWEALTH OF KENTUCKY — RESPONDENTS

AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, AND THE AMERICAN CIVIL LIBERTIES UNION OF KENTUCKY IN SUPPORT OF THE WRIT PETITION OF PETITIONERS VICSBINGO.COM AND INTERACTIVE GAMING COUNCIL

Respectfully submitted,

David A. Friedman, General Counsel
William E. Sharp, Staff Attorney
ACLU of Kentucky
315 Guthrie Street, Suite 300
Louisville, KY 40202
Phone: (502) 581-9746
Fax: (502) 589-9687

Attorneys for Amici Curiae

On the brief:

Matthew Zimmerman, Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San, Francisco, CA 94110
Phone: (415) 436-9333 (x127)
Fax: (415) 436-9993

John B. Morris, Jr., General Counsel
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
Phone: (202) 637-9800
Fax: (202) 637-0968

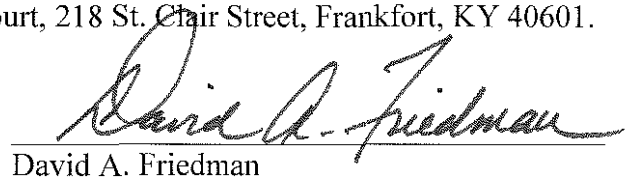
CERTIFICATE OF SERVICE

I hereby certify that I have served copies of this document by mailing copies, first class postage prepaid, on November 12, 2008, to: D. Eric Lycan, William H. May III, William C. Hurt, Jr., HURT, CROSBIE & MAY, PLLC, 127 Main Street, Lexington, KY

(*continued on back of cover*)

(*continued from front of cover*)

40507; Robert M. Foote, Mark Bulgarelli, FOOTE, MEYERS, MIELKE & FLOWERS, LLC, 28 N. First Street, Suite 2, Geneva, IL 60134; Lawrence G. Walters, WESTON, GARROU, WALTERS & MOONEY, 781 Douglas Avenue, Altamonte Springs, FL 32714; P. Douglas Barr, Palmer G. Vance II, Alison Lundergan Grimes, STOLL KEENON OGDEN PLLC, 300 W. Vine Street, Suite 2100, Lexington, KY 40507; William E. Johnson, JOHNSON, TRUE & GUARNIERI, LLP, 326 W. Main Street, Frankfort, KY 40601; John L. Krieger, Anthony Cabot, LEWIS & ROCA LLP, 3993 Howard Hughes Parkway, Suite 600, Las Vegas, NV 89169; Patrick T. O'Brien, GREENBERG TRAURIG, LLP, 401 E. Las Osas Blvd., Suite 2000, Ft. Lauderdale, FL 33301; Kevin D. Finger, Paul D. McGrady, GREENBERG TRAURIG, LLP, 77 W. Wacker Drive, Suite 2500, Chicago, IL 60601; Timothy B. Hyland, STEIN, SPURLING, BENNETT, DE JONG, DRISCOLL & GREENFEIG, P.C., 25 W. Middle Lane, Rockville, MD 20850; Michael R. Mazzoli, COX & MAZZOLI, 600 W. Main Street, Suite 300, Louisville, KY 40202; Merrill S. Schell, David A. Calhoun, WYATT, TARRANT & COMBS, LLP, 500 W. Jefferson Street, Suite 2800, Louisville, KY 40202; Phillips S. Corwin, Ryan D. Israel, BUTERA & ANDREWS, 1301 Pennsylvania Avenue, N.W., Suite 500, Washington, DC 20004; John L. Tate, Ian T. Ramsey, Joel T. Beres, STITES & HARBISON, PLLC, 400 W. Market Street, Suite 1800, Louisville, KY 40202; Bruce F. Clark, STITES & HARBISON, PLLC, 421 W. Main Street, P. O. Box 634, Frankfort, KY 40602-0634; A. Jeff Ifrah, Jerry Stouck, GREENBERG TRAURIG, LLP, 2101 L Street, NW, Suite 1000, Washington, DC 20037; and Hon. Thomas D. Wingate, Franklin Circuit Court, 218 St. Clair Street, Frankfort, KY 40601.



David A. Friedman

STATEMENT OF POINTS AND AUTHORITIES

I. INTRODUCTION

Amici curiae the Electronic Frontier Foundation ("EFF"), the Center for Democracy and Technology ("CDT"), and the American Civil Liberties Union of Kentucky ("ACLU of Kentucky") respectfully urge this Court to grant Viscbingo.com and the Interactive Gaming Council ("IGC")'s Writ Petition of October 28, 2008, and vacate the trial court's Order of October 16, 2008, which purported to seize the domain names of 141 Internet domain names pointing to websites operating on Internet web servers around the globe. Judge Wingate's Order (a) raises serious First Amendment concerns, (b) violates the Commerce Clause of the U.S. Constitution, and (c) is otherwise unenforceable as the trial court does not have jurisdiction over the domain name registrars who were ordered to transfer the domain names at issue. If allowed to stand, the Court's flawed Order would needlessly create uncertainty about the basic rules governing the operation of the Internet as well as the authority of courts both inside and outside of the United States to affect behavior in other jurisdictions. Moreover, if carried to its logical conclusion, the trial court's Order could well impose literally billions of dollars of additional costs on individuals and businesses throughout the world that have no significant contacts with Kentucky. *Amici* take no position on the substance or legality of the gambling websites that would be affected by the domain name seizure but instead file this brief to underscore the Order's lack of merit as well as the substantial damage that would result from Judge Wingate's flawed central premise – that website operators the world over have an affirmative duty to block visitors from visiting their sites on the basis of local rules, and that Kentucky courts can reach outside the state's borders to seize the domain names of entities that do not comply with this edict.

II. BACKGROUND

On October 16, 2008, Franklin Circuit Court Judge Wingate affirmed his previous Order of September 18, 2008, which ordered the seizure of over 100 Internet domain names that purportedly (a) constituted illegal "gambling devices" prohibited by Kentucky

law, and (b) that refused to impose "geographic blocks" to prevent Internet users in Kentucky from accessing any of the material on the sites to which the domain names currently point. *See* Order at 39-40. As discussed below, Judge Wingate's Order is not only unconstitutional and unlawful but also rests on incorrect factual assumptions.

As Petitioners explain, the distinctions between "websites," "IP addresses," and "domain names" are critical to the proper application of the law here. A "website" is "a collection of Web pages, images, videos or other digital assets that is hosted on one or more web servers."[1] An "IP address" is a unique, numerical number – like "89.2.164.31" or "222.34.1.4" – assigned to every web server or other computer connected to the Internet that functions much like a street address or telephone number for the computer to which it is assigned.[2] A domain name is an easy-to-remember alphanumeric text representation (often a word or phrase) that is linked through the "domain name system" to the numeric IP Address where a website is actually located.[3] A series of domain name servers contain massive databases, listing the proper IP address for each domain name.[4]

Thus, to analogize to the "real world," a website is akin to a building, such as the Grand Theater in Frankfort. An IP address is like the address of the building, "308 St. Clair Street, Frankfort, KY," while the domain name is the commonly known way to refer to the building – the words "Grand Theater" in this example. Finally, the "domain name system" is like a "Yellow Pages" directory that one can use to look up "Grand Theater" and learn that it is located at "308 St. Clair Street, Frankfort, KY." Both "Grand

---

[1] *See* "Website." Wikipedia. November 10, 2008. <http://en.wikipedia.org/wiki/Website>.

[2] *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409-410 (2d Cir. 2004). *See also* Writ Petition of Vicsbingo.com and Interactive Gaming Council of October 28, 2008 ("Writ Petition") at 21.

[3] *See Register.com, Inc.*, 356 F.3d at 410; Writ Petition at 21. *See also Peterson v. National Telecommunications and Information Admin.*, 478 F.3d 626, 629 (4th Cir. 2007) (describing domain name system) and "Domain Name System." Wikipedia. November 10, 2008. <http://en.wikipedia.org/wiki/Domain_name_system>.

[4] *See Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573, 577 (2d Cir. 2000) (describing the domain name server system in detail).

Theater" and "308 St. Clair St., Frankfort, KY" accurately refer to the same building in different ways, but one is easier for humans to remember.

The court's seizure of the domain names in this case is akin to ordering the Yellow Pages company to erase the accurate listing for "Grand Theater" (which points visitors to "308 St. Clair St., Frankfort, KY") and instead point visitors to a different address. Although this misdirection may be of little consequence to those who know their way around Frankfort, it is of huge consequence on the Internet, where there are literally billions of different web pages and the "addresses" are in numeric forms (such as "216.97.231.225" or "205.204.132.139") that have no meaning to most human visitors. An accurate appreciation of what domain names are and how they function is important to understand the First Amendment and Commerce Clause implications of the court ordering the seizure of domain names.

III. ARGUMENT

A. The Trial Court's Order is Overbroad and Would Infringe the First Amendment Interests of the Domain Name Owners as Well As the Public at Large.

Any order purporting to transfer domain name registrations from registrants to the Commonwealth of Kentucky raises serious First Amendment concerns because it would necessarily impede access to material that is legal not only in Kentucky but throughout the country and the world. Moreover, it would chill speech of all types, not simply the speech directly at issue in this case.

As conceived by Judge Wingate, domain names would be subject to seizure – and therefore can be disabled so that they will no longer correctly correlate to their respective intended sites' IP address – if the site enables behavior that is arguably illegal in Kentucky but may be legal elsewhere. Conversely, the court noted that for any of the domain names at issue "which are providing information only, the Seizure Order must be appropriately rescinded" (but even then the court placed the burden on the domain name owners to prove these facts at a forfeiture hearing). Such a ruling turns First Amendment

protections on their head. Third-parties who may wish to access such (legal) information, including *amici* and their constituents, would be prohibited from doing so if the court's Order is not rescinded.

Critically, there is nothing in the court's analysis that would limit its application to gambling domains. Under the court's theory, Kentucky would be able to seize *any* domain name, from anywhere in the world, that pointed to a website that Kentucky deemed to violate a local law. The court's jurisdictional theory literally puts speakers and publishers the world over – not to mention those who otherwise provide information regarding the location of sites on the Internet, such as by simply linking to them – at risk. The trial court's global reach for extra-territorial jurisdiction over the Internet cannot withstand First Amendment scrutiny.

First, as discussed above, "domain names" are nothing more than alphanumeric text representations that point to the IP addresses of the computer servers that host websites (like a phone book, which correlates a person's name with a phone number, or a map, which provides directions to a particular street address). Because the seizure Order demanded the transfer of domain name control, it implicates the ability of Internet users to access *any* of the content on the websites to which those domain names point, not just to the content to which the Commonwealth of Kentucky (and the trial court) object. For this reason alone, the Order is massively overbroad and unconstitutional. *See, e.g., Tory v. Cochran*, 544 U.S. 734, 736 (2005) (citing *Carroll v. President and Comm'rs of Princess Anne*, 393 U.S. 175, 183-84 (1968), for the proposition that an "order" issued in "the area of First Amendment rights" must be "precis[e]" and narrowly "tailored" to achieve the "pin-pointed objective" of the "needs of the case"); *Madsen v. Feminist Women's Health Clinic*, 512 U.S. 753, 765-66 (1994) (injunction may burden no more speech than necessary).

Second, regardless of whether domain names constitute "property" or not, the trial court's Order was based purely on the truthful speech inherent in the domain names in

question. Hardly amounting to "virtual keys for entering and creating" allegedly illegal materials (Order at 23), domain names are more accurately conceived of as maps or street signs, providing factual information regarding the location – the unique IP address – associated with a computer server. *See, e.g.,* George C.C. Chen, *A Cyberspace Perspective on Governance, Standards and Control*, 16 J. Marshall J. Computer & Info. L. 77, 113 (1997) ("The domain name is similar to a street sign in the real world, indicating the location of the Internet merchant and the nature of his business."); *Shell Trademark Mgmt. BV v. Canadian AMOCO*, No. 02-01365, 2002 U.S. Dist. LEXIS 9597, at *10-11 (N.D. Cal. May 21, 2002) (analogizing domain names to road signs).

As the court's Order targets the domain names at issue solely because of the truthful content of the speech contained in the domain name registry (the identification of a corresponding IP address), it is no different from a hypothetical order prohibiting domain name registrars from passing out leaflets telling potential viewers how to access the sites in question. That plainly would violate the First Amendment (*Organization for a Better Austin v. Keefe*, 402 U.S. 415 (1971)), and so does the trial court's Order here. Accordingly, like the injunction against leafleting overturned in *Organization for a Better Austin*, a seizure Order rendering the domain name inoperable would be a classic prior restraint, "the most serious and the least tolerable infringement on First Amendment rights." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976).

Moreover, because content on an Internet server can readily be changed, the permanent seizure of a domain name continues to impede access to speech even if the content changes so that it no longer violates any Kentucky law. *See, e.g., Center For Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004) (holding that statute requiring the blocking of access to particular domain names and that IP addresses be blocked amounted to an unconstitutional prior restraint (citing *Vance v. Universal Amusement Co.*, 445 U.S. 308 (1980) (overturning a permanent injunction against a movie theater)).

Not only are the First Amendment rights of domain name registrars harmed by the seizure of domain names on the ground that they point to foreign websites where the content of those sites is legal, the First Amendment rights of Internet users are affected as well. As the Supreme Court has repeatedly held, the First Amendment not only "embraces the right to distribute literature," it also "necessarily protects the right to *receive* it." *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943); *accord Board of Education v. Pico*, 457 U.S. 853, 867 (1982) ("the right to receive ideas is a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom") (emphasis in original); *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972) (First Amendment encompasses "right to receive information and ideas"); *Red Lion Broadcasting Co. v. F.C.C.*, 395 U.S. 367, 390 (1969) ("It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences which is crucial here. That right may not constitutionally be abridged ..."); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas"); *Lamont v. Postmaster General*, 381 U.S. 301, 308 (1965) ("The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers") (Brennan, J., concurring).

This Constitutional right to receive information applies specifically to information disseminated over the Internet. *See, e.g., Clement v. California Dept. of Corrections*, 364 F.3d 1148, 1150 (9th Cir. 2004) (holding that alleged that Pelican Bay State Prison violated the First Amendment rights of an inmate by prohibiting inmates from receiving material downloaded from the Internet); *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (invalidating law that restricted adults' right to access information on the Internet). Indeed, the First Amendment protection for Internet speech applies specifically to domain names themselves. *Taubman Co. v. Webfeats*, 319 F.3d 770, 778 (6th Cir. 2003) ("the

domain name is a type of public expression, no different in scope than a billboard or a pulpit"). Accordingly, the trial court's overbroad seizure Order compelling domain name registrars to transfer domain names to the Commonwealth of Kentucky implicates the First Amendment interests of the general public in receiving documents and information through the use of the identified domain names to find the IP addresses of particular businesses.

The Justice and Public Safety Cabinet may assert that some or all of the documents and information available through the targeted domain names remain available to the public using foreign domain names other than those at issue here, or by typing in the site's IP addresses directly. However, this merely proves the pointlessness of, and thus the lack of constitutionally adequate justification for, the court's blunt seizure Order. *See, e.g., Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 564 (1980) (law that restricts speech "may not be sustained if it provides only ineffective or remote support for the government's purpose").

Nor can the availability of alternate routes to the websites at issue compromise *amici*'s First Amendment rights in obtaining access to those sites through the specific domain names here. The Supreme Court has repeatedly held that "one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised elsewhere." *Schneider v. New Jersey*, 308 U.S. 147, 163 (1939); *accord Reno v. ACLU*, 521 U.S. 844, 879-80 (1997) (rejecting the government's contention that content-based restriction on speech in numerous Internet modalities was permissible because the law allowed a "reasonable opportunity" for such speech to occur elsewhere on the Internet; citing *Schneider*, the Court noted that "[t]he Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books."); *Va. State Bd. of Pharmacy*, 425 U.S. at 757 n.15 ("We are aware of no general principle that the freedom of speech may be abridged when the speaker's listeners could come by his message by some other means . . .");

Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 556 (1975) (holding an otherwise impermissible prior restraint against performance of musical "Hair" is not saved by availability of other forums for production). It is equally immaterial if the seizure order's only effect was to delay, rather than completely frustrate, access to the corresponding websites. *See Elrod v. Burns*, 427 U.S. 347, 373 (1976) ("The loss of First Amendment freedoms, even for minimal periods of time, constitutes irreparable injury").

B. A Geolocation Filtering Requirement Could Dramatically Increase the Cost of Operating a Website, Likely Driving a Significant Numbers of Sites Out of Business Worldwide.

The First Amendment deficiencies of the court's Order are in no way avoided by the additional imposition of an alternative Internet-wide "geographic filtering" requirement; indeed, the requirement compounds the problem. Not only does the requirement run afoul of the Commerce Clause (as discussed below), it would impose enormous and chilling burdens on lawful websites around the world. And in any event, the "geographic filtering" technology simply does not work well enough to afford any website legal protection from the asserted long arm of the Kentucky trial court.

In its Order, the court makes the remarkable assertion that the 141 Domain Names have been "designed" to reach Kentucky residents because the owners of those domain names could, if they "so chose," "filter, block and deny access to a website on the basis of geographic locations." Order at 24. "There are software that are available, which can provide filtering functions on the basis of geographical location, *i.e.*, geographical blocks." *Id.* No evidence is cited to support the court's findings or its striking conclusion that every operator of every website that fails to filter by location therefore affirmatively "targets" Internet users in Kentucky or consequently that the domain names used by such operators may be subject to seizure in every jurisdiction worldwide.

Even a cursory examination of factual findings by other courts cast serious doubt's on the trial court's theory and strongly indicates that server-side filtering is not a realistic option with which to comply with such a legal mandate:

• *Filtering is not 100% accurate*. First, due to the nature of various methods of connecting to the Internet (including, but not limited to, proxy servers, satellite connections, and other large corporate proxies), it is simply not possible to guarantee that website visitors are from a particular city, state, or even country. *See, e.g., American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) ("A product that Quova markets can determine, within a 20 to 30 mile radius, the location from which a user is accessing a Web site through a proxy server, satellite connection, or large corporate proxy. … The fact that Quova can only narrow down a user's location to a 20 to 30 mile radius results in Quova being unable to determine with 100 percent accuracy which side of a city or state border a user lives on if the user lives close to city or state borders.") (internal citations omitted). In addition, the ability to "geo-locate" users of large Internet service providers ("ISPs") like AOL drops even further because these ISPs route traffic through centralized proxies that identify the source of browser requests not as the location of the individual Internet user but as the location of the proxy server itself, which may or may not be anywhere close to the Internet user. *See, e.g., id.* ("If a visitor is accessing a Web site through AOL, Quova can only determine whether the person is on the East or West coast of the United States.").[5]

Moreover, the ability to accurately identify the geographic location of users is further diminished by the growing use of anonymizing proxy services such as those provided by companies by anonymize.com and by peer-to-peer technologies such as Tor. *See, e.g.,* Anonymize.com (located at http://www.anonymize.com), Tor (located at http://www.torproject.com). Using these services, it is trivially easy for a user in Kentucky to evade any "geolocation filtering" a website might use, and thus no website can confidently use such services to prevent access from Kentucky.

---

[5] Bamba Gueye, *et. al.*, *Investigating the Imprecision of IP Block-Based Geolocation*, in *Lecture Notes in Computer Science* Vol. 4427 237, 240 (Springer Berlin, Heidelberg 2007) *available at* http://www.nas.ewi.tudelft.nl/people/Steve/papers/Geolocation-pam07.pdf (finding "large geolocation errors" in technology that claimed to be able to identify the location of Internet users).

• *Filtering would impose significant cost on website operators*. Critically, the location services that the trial court asserts can be used are *not* built into the Internet or available to all websites. On the contrary, they are very expensive. One service that provides geolocation services, recently cited by the Eastern District of Pennsylvania, estimated that the cost of such services "can cost anywhere from $6,000 to $500,000 a year." *ACLU v. Gonzales*, 478 F.Supp.2d at 807.

Applying the court's analysis to its logical conclusion – that every operator of every website in the world may be found liable for infractions of local laws even though the site material may be legal in the jurisdiction(s) in which the operator, server, and domain name registrar are located – dramatically increases the sites' ongoing operational costs. Apart from the starkly higher legal compliance costs that such a rule would impose (associated with determining which laws of which of the world's 195 countries might apply to a given site's content), the collective cost associated with the technological implementation of such filters could – conservatively – be in the tens of billions of dollars *per year* (and this figure assumes that only 10% of world's active websites[6] used the service and the average annual total of *all* implementation costs was equal to the lowest amount cited above for the cost of the filtering technology alone). Given the percentage of small and/or non-commercial sites on the Internet whose owners would likely find a mandate to filter browsers from every jurisdiction in the world that may argue that the sites' content is illegal where it is viewed, the global makeup of Internet content would be invariably changed for the worse.

C. The Trial Court's Order Violates the Commerce Clause.

Under the trial Court's overly expansive jurisdictional theory, Kentucky courts would be authorized to seize any Internet domain name that linked to content deemed illegal under Kentucky law. Kentucky thus would be able to globally disable any

[6] *See, e.g.,* Netcraft.com 2008 Web Server Survey, available at http://news.netcraft.com/archives/2008/10/29/october_2008_web_server_survey.html, estimating that the number of active websites in the world is currently over 65 million.

website, thereby imposing its laws on the other 49 states and on the rest of the world. The Commerce Clause of the U.S. Constitution will not tolerate this exertion of authority, because it prohibits individual states from regulating "Commerce with foreign Nations, and among the several States." U.S. Const. art. I, § 8. By authorizing the seizure of domain names, the Commonwealth and trial court are attempting to do just that – regulate interstate and foreign commerce.

In one of the leading cases applying the Commerce Clause to the Internet, a federal district court explained:

> The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. *The Internet represents one of those areas*; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.

American Library Association v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) (emphasis added). Numerous cases across the country have applied the Commerce Clause to strike down attempted state burdens on Internet communications. *See, e.g., Cyberspace Communications, Inc. v. Engler*, 55 F. Supp. 2d. 737, 752 (E.D. Mich. 1999), *aff'd*, 238 F.3d 420 (6th Cir. 2000) (finding Commerce Clause violation because state regulation "would subject the Internet to inconsistent regulations across the nation").

Congress has legislated in the area of Internet gambling, *see* 31 U.S.C. § 5361 *et seq.*, but it specifically did not empower the states to regulate Internet gambling. *See id.* §§ 5361(b), 5262(10)(D)(ii) (neither extending nor preempting state laws). Thus, any state regulation of Internet gambling that has any impact outside of the state (as almost all Internet regulations would) is governed pursuant to an ordinary Commerce Clause analysis. And under the Commerce Clause, it is simply not permissible for Kentucky to prohibit access by residents of Las Vegas, for example, to access a site that is lawful in Nevada. Yet the trial court's Order represents just such an exertion of authority.

Beyond the interstate implications of a Kentucky seizure of domain names, such action would directly implicate the United States' foreign relations with the rest of the world, a subject that the Commerce Clause specifically reserves to the national government. Indeed, the United States has *already* been penalized by the global World Trade Organization for its discriminatory treatment of online gambling (in which some forms of gambling are permitted and some are not). *See* Decision, World Trade Organization, WT/DS285/R ("United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services"), Nov. 10, 2004 (available at http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm). An action by Kentucky to disable *global* access to *any* domain name (gambling or otherwise) would have a direct and concrete impact on the United States' trade and diplomatic relations with the rest of the world.

This Commerce Clause analysis connects directly to the free speech and civil liberties concerns discussed above. While the Kentucky trial court may attempt to seize domain names for alleged violations of local gambling regulations, other countries (ones that do not enjoy First Amendment protections) may choose to seize the domain names of foreign websites based (for example) solely on their expressive content. China, for example, may be very happy to follow Kentucky's lead by seizing the domain names of U.S. websites that promote religions that China bans. Even Western nations such as France have attempted to censor U.S.-located content that is completely lawful and constitutionally protected in this country. *See, e.g., Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 433 F.3d 1199 (9th Cir. 2006) (case arising out of France's efforts to censor content on Yahoo.com). Under the trial court's jurisdictional theory, the French court in the *Yahoo!* case would not need to take action directly against the Yahoo! company (as the French in fact did) – instead, it would simply seize the "yahoo.com" domain name. While the trial court may believe that the impact of its Order is limited,

the principle it articulates is one that threatens to undermine crucial legal principles that have prevented jurisdictions from attempting to assert such authority in the past.

D. The Trial Court Has Not Established – and Cannot Establish – That It Has Jurisdiction Over Domain Name Registrars Outside of Kentucky.

The trial court's Order is further deficient in that the court failed to consider – and indeed does not have – jurisdiction over the registrars, the entities with which the owners registered their domain names. While the trial court held that minimum contacts existed between Kentucky and the owners of the sites to which all 141 domain names direct Internet browsers (*see* Order at 19-21) (a dubious finding that the Petitioners properly challenge), the court never opined on any minimum contacts with the registrars themselves, the entities who received the court's Order to transfer the domain names.

The trial court purported to seize domain names pursuant to *in rem* jurisdiction over the domain names themselves (authority effectively contested by Petitioners in their writ application (*see* Writ Petition at 9-13)), but the seizure Order is necessarily directed at out-of-state registrars, *i.e.*, entities over which the court must have *in personam* jurisdiction. *See, e.g., Shaffer v. Heitner*, 433 U.S. 186, 207 (1977) ("[I]n order to justify an exercise of jurisdiction *in rem*, the basis for jurisdiction must be sufficient to justify exercising 'jurisdiction over the interests of persons in a thing.'"). And while the court perhaps concludes (indirectly) that its exercise of personal jurisdiction over out-of-state registrars would satisfy the "minimum contacts" test mandated by the Due Process Clause as articulated by the Supreme Court in *International Shoe v. Washington*, 326 U.S. 310 (1945), it makes no explicit findings to that effect, and it further fails to cite any *statutory* authority that would grant Kentucky courts the authority to exercise jurisdiction to the full extent permissible under the Due Process clause.

Pursuant to Kentucky's long-arm statute, no such jurisdiction exists. Under KRS § 454.210, a court may only exercise long-arm jurisdiction against tort-feasors, under certain circumstances, and "only a claim arising from acts enumerated in this section may

be asserted against him." KRS § 454.210(2)(b). No explicit statutory authorization exists to assert personal jurisdiction over foreign domain name registrars solely because they may "purposefully avail[] [themselves] of the privilege of conducting activities" within Kentucky (*see Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985)); rather, the legislature must affirmatively grant that authority. *See, e.g., Davis H. Elliot Co. v. Caribbean Utilities Co.*, 513 F.2d 1176, 1179 (6th Cir. 1975) (applying Kentucky law) ("The basic inquiry as to the validity of asserted *in personam* jurisdiction is a two-fold one which requires (1) a determination of whether the state legislature has authorized the courts of the state to exercise jurisdiction over the nonresident in question, and (2) a determination of whether the jurisdiction so authorized is consistent with Fourteenth Amendment due process as that concept is delineated in the 'minimum contacts' formula of *International Shoe Co. v. Washington* ..."); *Auto Channel, Inc. v. Speedvision Network, LLC*, 995 F. Supp. 761, 764 fn. 3 (W.D. Ky. 1997) ("The fact that the requirements of K.R.S. 454.210(2)(a) are theoretically satisfied by the same minimum contacts required by due process should not be taken to mean that the long-arm statute is superfluous ... [I]t is possible to decline jurisdiction based only on the language of the statute, without recourse to a due process analysis.").

As it was not authorized by any Kentucky statute, the trial court's seizure Order is *ultra vires* and unenforceable, regardless of whether or not any out-of-state registrar complied with it.[7]

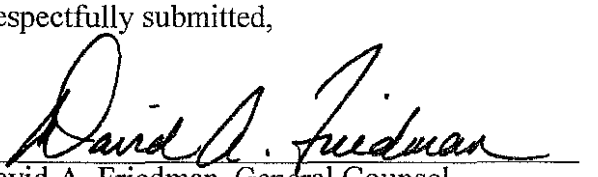
---

[7] As the trial court did not have jurisdiction over the domain name registrars that it purportedly "ordered" to transfer the domain names in question, registrars that complied with the court's Order, in whole or in part, may have violated their contractual obligations to their domain name customers. *See, e.g.,* GoDaddy.com's "Uniform Domain Name Dispute Resolution Policy" at <http://www.godaddy.com/gdshop/legal_agreements/show_doc.asp?plvid=1&pageid=uniform_domain> ("We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances: [including] our receipt of an order from a court or arbitral tribunal, *in each case of competent jurisdiction*, requiring such action. ... We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided ... above.") (emphasis added).

IV. CONCLUSION

The trial court's Order of October 16, 2008, purporting to seize the domain names associated with over 100 websites was, quite simply, unconstitutional and made without jurisdictional authority. *Amici* strongly urge this Court to vacate the trial court's Order, and order the Franklin Circuit Court to dismiss the case for lack of jurisdiction, and that the Circuit Court be directed to take those steps necessary to return the parties, and the domain names, to the status quo prior to the trial court litigation.

Respectfully submitted,



David A. Friedman, General Counsel
William E. Sharp, Staff Attorney
ACLU of Kentucky
315 Guthrie Street, Suite 300
Louisville, KY 40202
Phone: (502) 581-9746
Fax: (502) 589-9687
Email: dfriedman@ffgklaw.com

On the brief:

Matthew Zimmerman
Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Phone: (415) 436-9333 (x127)
Fax: (415) 436-9993
Email: mattz@eff.org

John B. Morris, Jr.
General Counsel
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
Phone: (202) 637-9800
Fax: (202) 637-0968 fax
Email: jmorris@cdt.org

Attorneys for Amici Curiae