SUPREME COURT OF KENTUCKY
NO. 2009-SC-000043

COMMONWEALTH OF KENTUCKY
J. MICHAEL BROWN, SECRETARY, JUSTICE
AND PUBLIC SAFETY CABINET — APPELLANT

v.

INTERACTIVE MEDIA ENTERTAINMENT & GAMING
ASSOCIATION, INC., *et. al.* — APPELLEES

ON APPEAL FROM
COURT OF APPEALS
ORIGINAL ACTION NOS. 2008-CA-002000, 2008-CA-002019, and 2008-CA-002036

AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE AMERICAN CIVIL LIBERTIES UNION OF KENTUCKY, THE MEDIA ACCESS PROJECT, THE UNITED STATES INTERNET INDUSTRY ASSOCIATION, THE INTERNET COMMERCE COALITION, AND THE INTERNET COMMERCE ASSOCIATION IN OPPOSITION TO THE APPEAL OF THE COMMONWEALTH OF KENTUCKY

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 April 17, 2009, to: D. Eric Lycan, William H. May III, William C. Hurt, Jr., HURT, CROSBIE & MAY, PLLC, 127 Main Street, Lexington, KY 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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

STATEMENT OF POINTS AND AUTHORITIES

I. INTRODUCTION AND BACKGROUND

Amici curiae the Electronic Frontier Foundation ("EFF"), the Center for Democracy and Technology ("CDT"), the American Civil Liberties Union of Kentucky ("ACLU of Kentucky"), the Media Access Project ("MAP"), the United States Internet Industry Association ("USIIA"), the Internet Commerce Coalition ("ICC"), and the Internet Commerce Association ("ICA") respectfully urge this Court to affirm the January 20, 2009, Writ of Prohibition ("Writ") granted by the Court of Appeals.

Collectively, amici are the leading public interest groups focused on civil liberties in the online environment, joined by a number of the leading trade associations representing the Internet industry. Together we urge this Court to give careful consideration to the constitutional and legal issues raised below. While the Court of Appeals correctly held that domain names were not "gambling devices" under KRS § 528.020, the trial court's order of October 16, 2008, ("Order") was further deficient in at least five respects: it (a) infringed fundamental First Amendment principles; (b) violated the Commerce Clause of the U.S. Constitution; (c) misread the statute to conflict with – and face preemption under – the federal Communications Decency Act; (d) violated the due process rights of the out-of-state registrars ordered to transfer the domain names because the trial court cannot exercise personal jurisdiction over them; and (e) imposed unrealistic and potentially devastating burdens on the domain names' owners.

As a threshold matter, it is essential to reiterate the distinctions between "websites," "IP addresses," and "domain names." A "website" is "a collection of related web pages, images, videos or other digital assets that is hosted on one web server."[1] An "IP address" is a unique, numerical sequence – 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

[1] *See* "Website." Wikipedia. April 12, 2009. http://en.wikipedia.org/wiki/Website.
[2] *See, e.g., Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409-410 (2d Cir. 2004).

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 40601," 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 40601." Both "Grand Theater" and "308 St. Clair St., Frankfort, KY" accurately refer to the same building in different ways, but the former is far easier for humans to remember.

The court's seizure of the domain names in this case is akin to ordering the publisher of the yellow pages to transfer ownership of the listing for "Grand Theater" (which points visitors to "308 St. Clair St., Frankfort, KY") to the Secretary so that he may (presumably) order it erased or point visitors to a different address. Although this misdirection may be of slight 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.

II. ARGUMENT

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

Reinstating the trial court's Order would raise serious First Amendment concerns because it would inevitably chill countless types of speech as well as impede access to material that is

---

[3] *See, e.g., Register.com, Inc.*, 356 F.3d at 410. *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. April 12, 2009. 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).

legal in Kentucky and other jurisdictions. According to the trial court, a domain name is subject to seizure if the website to which it directs visitors contains *some* material that is arguably illegal in Kentucky but may be legal elsewhere. At the same time, the trial court noted that the Order should not apply to any of the domain names "which are providing information only," but even then the court placed the burden on the domain name owners to prove these facts after seizure at a forfeiture hearing. Order at p. 21. Such a ruling does not comply with the requirements of the First Amendment.

Critically, there is nothing in the trial court's analysis limiting its application to domain names associated with online gaming. Under its theory, the court would be able to seize *any* domain name that directed visitors to a website that Kentucky deemed to violate a state law. That would literally (and impermissibly) put speakers the country and world over – including those who merely link to other websites – at risk.

First, as discussed above, "domain names" are nothing more than alphanumeric representations that point to the IP addresses of the websites' servers. By awarding the Secretary absolute control over the domain names, the trial court's Order jeopardized users' access to *any* of the content on the associated websites, not just to the content to which the Secretary objects. For this reason alone, the Order is massively overbroad and unconstitutional. *See, e.g., Tory v. Cochran*, 544 U.S. 734, 736 (2005) ("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') (quoting *Carroll v. President and Comm'rs of Princess Anne*, 393 U.S. 175, 183-84 (1968)).

Second, regardless of whether domain names constitute "property," the trial court's Order was based purely on the truthful speech inherent in the domain names in question. Domain names are not "virtual keys for entering and creating" allegedly illegal materials (Order at 23); rather, they are more accurately described as "a street sign in the real world, indicating the location of the Internet merchant and the nature of his business." George C.C. Chen, *A Cyberspace Perspective on Governance, Standards and Control*, 16 J. Marshall J. Computer &

Info. L. 77, 113 (1997); *see also 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 such, the First Amendment protection for Internet speech applies specifically to domain names themselves. *See Taubman Co. v. Webfeats*, 319 F.3d 770, 778 (6th Cir. 2003) ("[T]he domain name is a type of public expression, no different in scope than a billboard or a pulpit . . .").

The trial court's Order targets these domain names solely because of the truthful content of the speech contained in the domain name registry: the identification of corresponding IP addresses. It is therefore indistinguishable from an order prohibiting registrars from passing out leaflets telling potential viewers how to find the sites in question. Like the injunction against leafleting overturned in *Organization for a Better Austin v. Keefe*, 402 U.S. 415 (1971), 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, the permanent seizure of a domain name continues to impede access to speech even if the content changes so that it no longer arguably violates any Kentucky law. *See, e.g., Center For Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004) (holding that statute requiring the blocking of access to particular domain names and IP addresses amounted to an unconstitutional prior restraint) (citing *Vance v. Universal Amusement Co.*, 445 U.S. 308 (1980) (overturning a permanent injunction against a movie theater)).

Such an order would likewise impair the First Amendment rights of Internet users. 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). This Constitutional right to receive information applies specifically to information disseminated over the Internet. *See, e.g., Reno v. ACLU*, 521 U.S.

844, 874 (1997) (invalidating law that restricted adults' right to access information on the Internet). Accordingly, the trial court's overbroad seizure Order implicates the public's First Amendment interests in receiving documents and information through the use of the identified domain names to locate the IP addresses of particular sites.

The Secretary may assert that some or all of the information available through the targeted domain names remains available to the public using another domain name, or by typing in the site's numerical 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 does the possible availability of alternate routes to the websites compromise *amici*'s First Amendment rights to access those sites through the targeted domain names. 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*, 521 U.S. at 879-80 (rejecting argument 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); *Va. State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 757 n.15 (1976) ("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 . . .").

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

Under the trial court's jurisdictional theory, Kentucky courts would be authorized to seize any domain name that linked to any content deemed illegal under Kentucky law. Kentucky thus would be able to disable any website, thereby imposing its laws on the rest of the country and, indeed, the rest of the world. The federal Commerce Clause, however, 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 exactly what the Commerce Clause prohibits – regulate interstate and foreign commerce.

As a leading case applying the Commerce Clause to the Internet 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). Courts across the country have applied the Commerce Clause to strike down attempts by states to regulate or otherwise burden 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 the Internet with impact outside of the State (as almost all Internet regulations would) is subject to "dormant" Commerce Clause scrutiny. Under that analysis, Kentucky may not prevent, for example, a Las Vegas resident from accessing a site that is lawful in Nevada, or a New York resident from accessing that same Nevada site. Yet by seizing a domain name, the trial court's Order is preventing residents of Nevada, New York, and the world over from accessing the related website – an exertion of interstate and global authority that the Commerce Clause does not permit.

Beyond the interstate implications of a Kentucky seizure of domain names, such action would directly implicate the United States' foreign commerce, a subject specifically reserved to

the federal 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). Permitting Kentucky to disable *global* access to *any* domain name (gambling or otherwise), would directly affect the United States' trade and diplomatic relations.

If Kentucky can seize the domain names at issue here, other countries (which do not have our First Amendment) will no doubt seek to seize the domain names of websites – including websites based in the United States – solely because of their expressive content. Chinese officials, for example, would likely be happy to seize the domain names of U.S. websites that promote religions banned in China. Even Western nations such as France have attempted to censor U.S.-located content that is 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). 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. Under this approach, no website on the Internet would be safe from interference by any country that disagreed with the website's content.

C. Section 230 of the Communications Decency Act Immunizes Domain Name Registrars From Liability for Any State Criminal Act Performed by Their Customers, and It Preempts KRS § 528.020 to the Extent that Domain Names are "Gambling Devices."

The Secretary is badly mistaken in asserting that domain name registrars could be liable for the alleged criminal activities of their customers if they did not comply and transfer control of the domain names at issue in response to the trial court's erroneous Order: federal law immunizes "interactive computer services" providers such as domain name registrars precisely to protect them from the type of thinly-veiled threats made by the Secretary here. Section 230 of

the Communications Decency Act of 1996 – 47 U.S.C. § 230 ("CDA 230") – states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Contrary to the Secretary's assertions (Br. 47), the domain name owners have in no way exposed their registrars to potential legal liability vis-á-vis Kentucky law.

Domain name registrars are interactive computer service providers and enjoy the protections of CDA 230. *See, e.g., Smith v. Intercosmos Media Group, Inc.*, 2002 WL 31844907 (E.D. La. 2002). Courts have construed CDA 230 broadly, immunizing online providers from liability for a wide range of their customers' activities. *See, e.g.*, *Kathleen R. v. City of Livermore*, 87 Cal. App. 4th 684, 692 (2001) (city immune for public library's providing computers with access to pornography); *Green v. America Online (AOL)*, 318 F.3d 465 (3rd Cir. 2003) (immunity for AOL's failure to block computer program created by hacker to halt and disrupt another computer); *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003) (affirming immunity for hosting services provider against complaint of "unconsented" videos sold on the Internet). And while some actions are explicitly excluded from CDA 230's grant of immunity (such as intellectual property claims or *federal* criminal statutes), interactive computer services enjoy absolute protection from *state* criminal statutes based on their customers' actions. *See Voicenet Communications, Inc. v. Corbett*, 2006 WL 2506318 (E.D. Pa. 2006) (finding the "CDA confers a § 1983-enforceable right upon Internet service providers and users to not be 'treated' under state criminal laws as the publisher or speaker of information provided by someone else").

The protections of CDA 230 present yet another problem for the Secretary: if domain names are indeed "gambling devices" under KRS § 528.020, then CDA 230 would pre-empt the statute as to providers of "interactive computer services" such as registrars. *See* 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."). To the extent that the term "gambling device" is ambiguous as applied here, canons of statutory construction counsel the court to construe it to avoid the pre-emption of state law; *i.e.*, not to cover domain names. *See, e.g., State*

v. Mooney, 98 P.3d 420, 425 (Utah 2004) ("We . . . avoid interpreting an ambiguous state statute . . . [to] render the statute invalid under an explicitly preemptive federal law."); *Martin ex rel. Hoff v. Rochester*, 642 N.W.2d 1 (Minn. 2002) (holding that if a state statute "is susceptible to an alternative interpretation that allows it to operate in harmony with the federal [statutory] scheme and not be preempted, we must apply that interpretation."). If, however, the Court finds that "gambling device" plainly covers domain names, KRS § 528.020 is pre-empted.

D. The Trial Court's Order Requiring the Transfer of Domain Names From Out-of-State Registrars Over Whom the Court Lacks Personal Jurisdiction Violates the Requirements of Due Process.

The Commonwealth's attempt to seize domain names directly from out-of-state registrars is additionally flawed because it did not – and cannot – meet the requirements of due process. First, the domain name registrars ordered to transfer or lock the domain names at issue were not parties to the underlying action. As *amicus* Network Solutions noted in its brief before the Court of Appeals, "a person should not be bound by an injunction decree until she has had her day in court." *Lewis LP Gas, Inc. v. Lambert*, 113 S.W.3d 171, 175 (Ky. 2003)*; see also, e.g.*, *Zenith Radio Corp. v. Hazeltine Research, Inc.*, 395 U.S. 100, 112 (1969) ("It was error to enter the injunction against the [non-party], without having made this determination in a proceeding to which the [non-party] was a party."); *U.S. v. Kirschenbaum*, 156 F.3d 784, 795 (7th Cir. 1998) ("However convenient it might be for the government to violate the due process rights of some citizens in an effort to seize property that it contends is forfeitable, we see no way that it could do so."). Absent the participation as parties of the registrars whom the trial court sought to enjoin, its orders are void.

Second, the trial court cannot exercise personal jurisdiction over the registrars (necessary in any *in rem* forfeiture action) in this matter. Personal jurisdiction has both statutory and constitutional components. A court must first determine whether a statutory provision – *i.e.*, a long-arm statute – authorizes the exercise of extra-territorial power. A court must then determine whether that statutory authority complies with federal constitutional limitations. *See, e.g., Davis H. Elliot Co. v. Caribbean Utilities Co.*, 513 F.2d 1176, 1179 (6th Cir. 1975)

(applying Kentucky law). Here, the trial court purported to seize domain names pursuant to *in rem* jurisdiction over the domain names themselves, which as Appellees explained below (*see* Writ Petition of Vicsbingo.com and Interactive Gaming Council of October 28, 2008 ("Writ Petition") at 9-13), the trial court did not have. Moreover, because the seizure Order was directed at out-of-state registrars, it must have *in personam* jurisdiction over those entities to effect it. *See, e.g., Shaffer v. Heitner*, 433 U.S. 186, 207 (1977). While the court perhaps concluded (indirectly) that its exercise of personal jurisdiction over out-of-state registrars would satisfy the Due Process Clause's "minimum contacts" analysis, the court made no explicit findings to that effect. It also failed to cite any *statutory* authority that would grant Kentucky courts the authority to exercise such jurisdiction. In fact, no such statutory authority exists.

1. The Trial Court's Seizure Order Does Not Satisfy Kentucky's Long-Arm Statute, and In Any Case, the Trial Court Made No Findings That Would Satisfy Its Statutory and Constitutional Minimum Contacts Obligations.

Kentucky's long-arm statute simply does not grant the trial court personal jurisdiction over non-parties, nor could it consistent with the due process limitations discussed above. Under KRS § 454.210, a court may exercise long-arm jurisdiction only against *defendants* – not non-parties like the domain name registrars here – and only under certain circumstances. Moreover, "only a claim arising from acts enumerated in this section may be asserted against" a defendant. KRS § 454.210(2)(b). No statutory authorization exists to assert personal jurisdiction over foreign domain name registrars whose business in the state (if any) is not the subject of the underlying suit.

Even if Kentucky had a long-arm statute that authorized the exercise of personal jurisdiction over out-of-state non-parties, the trial court would still be obligated to determine "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*." *Davis H. Elliot Co.*, 513 F.2d at 1179. The trial court made no factual inquiry regarding any "minimum contacts" that the domain name registrars purportedly may possess.

2. The Cases Cited by the Secretary Demonstrate That Any Extra-Territorial Exercise of Personal or *In Rem* Jurisdiction Requires Authorizing Legislation and a Final Judgment.

The cases cited by the Secretary to support its argument that the trial court enjoyed "jurisdiction" over the domain name registrars are plainly inapposite. In every case the Secretary cites for the proposition that "extra-territorial forfeiture is consistent with due process" (Br. 35-37), the government sought to enforce a *final judgment* obtained pursuant to a federal statute (28 U.S.C. § 1355) explicitly granting subject matter jurisdiction as well as *in rem* jurisdiction over the foreign property at issue. Neither is the case here.

There may, of course, be means by which competent authorities can seize property *after* a valid final judgment is obtained. Under the Full Faith and Credit Clause, for example, the Secretary presumably could ask a court having personal jurisdiction over a registrar (and *in rem* jurisdiction over a domain name) to order compliance with a valid final judgment obtained in a Kentucky court. Similarly, as the cases cited in the Secretary's brief acknowledge, the Secretary could petition a foreign government that retains jurisdiction over a foreign registrar to enforce a final Kentucky state court judgment. *See, e.g., United States v. Certain Funds Located at the Hong Kong & Shanghai Banking Corp.*, 96 F.3d 20, 22 (2d Cir. 1996). What the trial court may *not* do, however, is exert extraterritorial power over an out-of-state entity necessary to effectuate the relief sought but over which it does not have personal jurisdiction.

3. The Contractual Agreement Between the Domain Name Registrars and the Domain Name Owners Does Not Indicate Consent to Jurisdiction in Kentucky, and Even If It Did, Neither the Secretary Nor the Trial Court May Invoke Such a Term.

The Secretary also erroneously asserts that the terms of the private contractual agreement between the domain name registrars and the owners of the domain names places the domain names "in the Court's constructive possession" because the registrars agreed (as part of a uniform contractual term mandated by the Internet Corporation for Assigned Names and Numbers (ICANN)) to transfer a domain name in the event that they receive such an order from a court "of competent jurisdiction." *See* ICANN Uniform Domain Name Dispute Resolution Policy ("UDRP") ¶ 3. While *amici* strongly disagree that the trial court is one "of competent

jurisdiction" (see above), that term is relevant only *between the contracting parties*. The Secretary has presented no evidence that it is a third party beneficiary to any of the registrar/owner agreements. Any "constructive possession" the trial court may now enjoy over any of the domain names exists (if at all) *solely* because of a voluntary decision by some of the registrars to transfer control of the domain names in response to the trial court's ruling.[5]

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

Finally, the deficiencies of the trial court's Order would be exacerbated – not remedied – by the imposition of an Internet-wide "geographic filtering" requirement. Such a requirement would both run afoul of the Commerce Clause (see pp. 6-7 *infra*) as well as impose enormous and chilling burdens on lawful websites around the world. In any event, the "geographic filtering" technology simply does not work well enough to afford websites legal protection from the asserted reach of the Kentucky trial court.

The trial court made 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," the court claimed, that "can provide filtering functions on the basis of geographical location, *i.e.*, geographical blocks." *Id.* The

[5] The Secretary badly misunderstands the private contractual terms set forth in the UDRP in other ways as well. The UDRP does not, contrary to the Secretary's insistence (Br. 46), mandate that registrars "cannot be brought into the action" because the UDRP supposedly mandates that a "registrar will not be made a party to any dispute between the registrant and a third party . . ." If only immunizing one's self against suits brought by third parties was as simple as declaring as much in a contract. The UDRP actually states that a *domain name owner* "shall not name [the registrar] as a party or otherwise include us in any such proceeding" involving a "dispute between you and any party other than us." UDRP ¶ 6. Moreover, the Secretary fails to note that this same paragraph specifically anticipates registrars being named in lawsuits involving third parties: "In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves." *Id.* The Secretary did not bring suit against the registrars based on any alleged contractual obligation of the registrars to the Commonwealth because no such obligation exists, not because the UDRP somehow prevents the Secretary from filing suit.

court cited no evidence, however, to support its striking conclusion that every operator of every website that fails to filter by location therefore affirmatively "targets" Internet users in Kentucky and that the domain names used by such operators are therefore subject to seizure in every jurisdiction worldwide.

A brief review of factual findings rendered by other courts casts serious doubt on the trial court's assumption that server-side filtering is a realistic option:

• *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) ("The fact that [location software] can only narrow down a user's location to a 20 to 30 mile radius results in [that software] 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 by 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, [software] can only determine whether the person is on the East or West coast of the United States.").[6]

The ability to identify accurately the geographic location of users is further diminished by the growing use of anonymizing proxy services such as those provided by companies like anonymize.com and by peer-to-peer technologies such as Tor. *See, e.g.,* www.anonymize.com; www.torproject.com. These services make it trivially easy for a user to evade any "geolocation

[6] *See* 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" a website might use, and thus no website can confidently prevent access from Kentucky.

• *Filtering would impose significant costs on website operators*. Geolocation services are *not* built into the Internet or readily available to all websites. Indeed, they are very expensive. As one court recently observed, one geolocation provider estimated that the cost of such services could range "anywhere from $6,000 to $500,000 a year." *ACLU v. Gonzales*, 478 F. Supp. 2d at 807.

Carried to its logical conclusion, the trial court's analysis – *i.e.*, that operators of every website in the world are 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 websites' operational costs. Apart from the starkly higher legal compliance costs that such a rule would impose (associated with determining which laws of the world's 195 countries and their political subdivisions might apply to a given site), the cost of implementing such filters could – conservatively – be tens of billions of dollars *per year* (assuming that only 10% of world's 65 million active websites[7] used the service and the average annual total of *all* implementation costs was equal to the lowest amount cited above). Given the percentage of small and/or non-commercial sites on the Internet whose owners would likely be able to comply with a mandate to impose filters incorporating the laws of every jurisdiction in the world, the global makeup of Internet content would be invariably changed for the worse.

[7] *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.

III. CONCLUSION

This Court should affirm the Writ of Prohibition vacating the trial court's Order.

Respectfully submitted,

Date: April 17, 2009 By _____

David A. Friedman, Esq., General Counsel
William E. Sharp, Staff Attorney
ACLU OF KENTUCKY
315 Guthrie Street, Suite 300
Louisville, KY 40202
Telephone: (502) 581-9746
Facsimile: (502) 589-9768

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

Attorneys for *Amici Curiae* Electronic Frontier Foundation, the Center for Democracy & Technology, the American Civil Liberties Union of Kentucky, the Media Access Project, the United States Internet Industry Association, the Internet Commerce Coalition, and the Internet Commerce Association