

Nos. 01-15899 & 01-15886

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

GARY KREMEN,
Plaintiff-Appellee/Cross-Appellant,

v.

STEPHEN MICHAEL COHEN, an individual, OCEAN
FUND INTERNATIONAL, LTD., a corporation, YNATA
LTD., a corporation, SAND MAN INTERNACIONAL
LIMITED, S.A. de C.V., a corporation, and DOES 1-20,

Defendants-Appellants,

and

NETWORK SOLUTIONS, INC., a corporation,
Defendant-Cross-Appellee.

On Appeal From The United States District Court
For The Northern District Of California
The Honorable James Ware, Presiding

**BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF REVERSING THE DISTRICT COURT'S SUMMARY
JUDGMENT IN FAVOR OF NETWORK SOLUTIONS, INC.**

Robin Gross, Esq.
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 863-5459
Amicus Curiae

I. Statement of Interest

The Electronic Frontier Foundation (“EFF”) is a non-profit, civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. Founded in 1990, EFF is based in San Francisco. EFF has members all over the world and maintains one of the most linked-to Web sites (<http://www.eff.org>) in the world. EFF has an interest in this appeal because, as discussed below, the district court’s decision granting summary judgment in favor of Network Solutions, Inc. (“NSI”) sets a dangerous precedent of lack of accountability that could, if not reversed, seriously injure the rights to free expression that currently exist on the Internet.

EFF is filing this brief, pursuant to Rule 29 of the Federal Rules of Appellate Procedure, along with the attached Motion For Leave to File Brief of *Amicus Curiae*.

II. Summary of Argument

The Internet has, for the first time, made it possible for almost all citizens of the world community to freely share and develop information and ideas “as diverse as human thought.” *Reno v. ACLU*, 521 U.S. 844, 852 (1997). As the Supreme Court observed:

From a publisher’s standpoint, [the Internet] constitutes a vast platform from which to address and hear from a worldwide

audience of millions or readers, viewers, researchers and buyers
. . . . Through the use of chat rooms, any person with a phone
line can become a town crier with a voice that resonates farther
than it could from any soapbox. Through the use of web pages,
. . . the same individual can become a pamphleteer.

Reno v. ACLU, 521 U.S. at 853, 870.

Thus, although it is fundamentally made up of technology, the Internet is much more — it has become a critical resource for free expression that must be safeguarded for the public good.

While the use of the Internet is diverse, its core operations are currently centralized in a small number of “architecture” or “governance” organizations that maintain the Root Server, Domain Name System (DNS), and other related infrastructure and protocols that allow the Internet to function. These organizations have been given enormous powers to control the Internet and therefore have a corresponding responsibility to use those powers fairly.

By concluding that Network Solutions, Inc. (“NSI”) owed no duties to Gary Kremen when he registered his domain name and thus immunizing it from liability for even gross misconduct in its handling of domain names generally, the district court eliminated NSI’s most reliable incentive to act properly. It thereby left a key component of the Internet in the hands of a private organization that has no accountability to the Internet community to administer it fairly or reasonably.

That decision should not stand. NSI and the other core providers of Internet architecture have been given, improperly in EFF's view, monopoly power over a key portion of arguably the most important commercial and social system in the world. Under both established law and important public policy, these companies must be held responsible if they fail in their duties. If they are not, then the only thing standing between a functioning Internet and chaos are the "good intentions" of NSI and others like it. As the facts of this case demonstrate beyond cavil, good intentions are not enough. Not just for Kremen, but for the future functioning of the Internet, this Court should reverse the lower court's decision and find that NSI, like other companies, is accountable for failing to reasonably carry out its duties.

III. The Internet Benefits All of the World's Citizens

The technical details of the Internet have been described in numerous court opinions and other publicly available sources¹ and will not be repeated in detail here. The Internet is far more, however, than a sophisticated piece of technology; it is an unprecedented tool for global freedom. For the first time in history, practically any member of the human race with access to an inexpensive computer can exchange ideas, information, or art with anyone on the planet, and even astronauts circling above it. Beyond the individual level, the Internet offers

¹ See, e.g., *Reno v. ACLU*, 521 U.S. at 849-53.

traditionally disenfranchised groups throughout the world the opportunity for meaningful participation in global and local public debate.

Recognizing the substantial democratic and social value of the Internet, both courts and commentators have universally hailed it as potentially the most diverse and democratic communications medium the world has ever known. *See, e.g., ACLU v. Reno*, 929 F. Supp. 824, 881 (E.D. Pa. 1996) (opinion of Dalzell, J.); Eugene Volokh, *Cheap Speech and What It Will Do*, 104 Yale L.J. 1805, 1833-43 (1995). Indeed, the U.S. Supreme Court has praised the Internet as a “vast democratic forum[]” that is “open to all comers,” which has created a “new marketplace of ideas” with “content [that] is as diverse as human thought.” *Reno v. ACLU*, 521 U.S. at 868, 870, 880, 885.

The true value of the Internet is thus found not in its technological infrastructure, but in the diversity of its content and the concomitant expansion of human liberties that Internet access provides. This revolutionary resource cannot be controlled by any one person, one corporation, or even one country; it should be held in trust for current and future generations of humankind.

IV. Network Solutions and Other Internet Infrastructure Entities Have Been Given Substantial Technological Power Over the Internet

A. The Current “Architecture” of the Internet Is Based on a Small Number of Key Infrastructure Entities

Somewhat paradoxically, while the value of the Internet lies in decentralization and individual freedom, its “architecture” requires a uniform reference point. Just as sailors navigate the world’s oceans using a uniform system of longitude and latitude calculated from the original site of the Royal Greenwich Observatory at Greenwich, England, Internet users navigate the World Wide Web through a uniform system of IP addresses and corresponding domain names, all managed by the Domain Name System (DNS).²

The DNS, like most databases, is hierarchical. Under the DNS, all domain names are assigned to a top level domain “TLD” such as “.com” or “.org.” There are three types of TLDs: generic TLDs (like .com), which were created for use by the Internet public, restricted TLDs (like .mil) which were created for specific purposes, and country code TLDs, which were created to be used by each

² An IP (Internet Protocol) address is a series of four numerical segments, each of which has up to three digits, that identify computer networks within the Internet and specific computers within those networks (e.g., 204.253.162.3). Because these numeric addresses are difficult, if not impossible, to be easily used, domain names were created to facilitate easier, more widespread use of the Internet. Each domain name is associated with a specific IP address. The computer database system that correlates domain names with IP addresses is called the Domain Name System or DNS.

individual country. Persons or entities wanting to register a generic TLD domain name may now do so through one or more “registrars” who are accredited by ICANN, another key infrastructure entity,³ to register domain names in the applicable TLD. In addition, each TLD also has a “registry,” an entity that maintains the official records correlating domain names with IP addresses for all registrations in the TLD. A master database is necessary for the DNS to function, just as a uniform “zero longitude” reference point is required for a global system of navigation.⁴

B. As the “.Com” Registry and Custodian of Root Server A, NSI Has Been Given Unparalleled Control Over the Internet

In its decision, the district court in this action described NSI’s conduct as “innocently performing a purely ministerial function.” *Kremen v. Cohen*, 99 F. Supp. 2d 1168, 1174 (N.D. Cal. 2000). The court’s description reveals a

³ The Internet Corporation for Assigned Names and Numbers (ICANN) “coordinates the assignment of the following identifiers *that must be globally unique for the Internet to function*: [1] internet domain names, [2] IP address numbers, and [3] protocol parameter and port numbers. <http://www.icann.org>. North American IP addresses are allocated for use by the American Registry of Internet Numbers (ARIN), another Internet governance entity.

⁴ Although the current DNS architecture involves only one “registry” controlling the master database for each TLD, the same system would work with decentralized, multiple registries each of which were able to alter the master database according to a set of mutual agreements establishing such a system. Thus, while it is essential that there be a uniform reference point, it is not essential, nor is it beneficial, for control over that reference point to be vested in one entity as it is under the current scheme.

fundamental misunderstanding of NSI's function and the concomitant power NSI wields over the entire Internet.

Until 1999, NSI was the sole registrar of the “.com” TLD, the most populated TLD available to private use, along with other TLDs. At that time, NSI served the function of both registry and registrar for all “.com” domain names. In 1998, registration services in the .com TLD were expanded to include other registrars. However, NSI is still the registry for the .com TLD, and thus has sole, physical care, custody and control of the master domain name to IP address lookup database for all .com domain names.

As a result of its governmentally created monopoly, NSI developed and now controls the primary DNS Root Server, Root Server A. Root Server A contains the .com TLD registry. It also contains the IP addresses for the registries for all other TLDs in the world. Thus, if a computer user enters a domain name within Liechtenstein's country code TLD (“.li”), the DNS first checks Root Server A to determine the IP address of the “.li” TLD registry, and then consults that registry to determine the IP address of the domain name.

This is no insignificant role. While it may not be obvious at a first glance, the management of the Internet domain naming system impacts greatly on the fundamental human rights of free expression, free association, due process, and nondiscriminatory administration. It is through Internet protocol addresses and

domain names that individuals and organizations place their speech on the Internet and give titles to them or to collections of them, and it is through these addresses that others locate that speech to read and use it.

It is important to understand the staggering ability NSI has been given to manipulate Internet access through its control of the DNS. By simply changing an entry in its registry, NSI can effectively delete any “.com” website by making it impossible to find that site through its domain name. NSI is thus technologically able to silence almost any Internet voice it chooses. On a larger scale, because NSI maintains the database that coordinates IP addresses for all other TLD registries, including the country code TLDs, NSI has the ability to terminate Internet access for entire countries by changing or erasing the information associated with their TLDs. Other registries have similar power within the TLDs they oversee, as does ARIN, which controls the very assignment of IP addresses themselves in North America.

In the view of EFF and many other commentators, the United States government made a serious, and probably illegal, mistake by allowing NSI to exercise sole control over both the technical and policy decisions surrounding Root Server A and the registry for the .com TLD.⁵ As a result of this transfer of

⁵ A more thorough discussion of the dangers of private management of the DNS system, and the problems with NSI’s stewardship in particular, is set forth in

authority from the federal government to NSI, EFF and many others believe that NSI should be treated as a governmental — or at least quasi-governmental — entity rather than as a private corporation. Unfortunately, in exercising its power, NSI has often acted in its own interests rather than in the interests of the global public.

EFF has repeatedly warned that granting unchecked authority over key Internet functions to private corporations like NSI, and NSI in particular, presents a substantial risk to the public interest. This case presents a textbook example of the type of malfeasance EFF has repeatedly warned against, and it is far from the only example. EFF staff has advised numerous individuals with similar problems caused by NSI's mismanagement of the domain name system. While EFF believes that NSI should never have been given the control it has, at a minimum NSI must be accountable for its actions in the civil courts. By concluding that NSI is not even civilly responsible to those injured for its conduct in managing domain names, the district court erroneously eliminated any incentive NSI has to act consistent with the public good with which it has been entrusted.

EFF comments on the U.S. Department of Commerce's National Telecommunications and Information Administration proposal regarding future management of the Internet Domain Name System (DNS), available at www.eff.org/Infrastructure/DNS_control/19980323_eff_ntia.comments.

V. With Great Power Comes Great Responsibility

A. NSI, Like All Internet Infrastructure Entities Must Act Responsibly So That the Internet Will Function Fairly and Reasonably

Control over the DNS has a drastic impact on the basic human rights of free expression and free association: individuals and organizations can publish their speech on the Internet only through the use of domain names and IP addresses. Similarly, other persons must use those domain names or addresses to receive that speech. The ability to control the DNS is, at bottom, the ability to control or eliminate Internet speech.

In light of the power that key infrastructure entities like NSI have over the Internet, management of the DNS should not be left in the hands of unaccountable private entities. However, given that such organizations are currently entrusted with some of that management, they must be required to administer the DNS fairly, for the long term benefit of Internet users, the general public, and indeed the entire human race. NSI was not granted its substantial position of power over the Internet in order to wield it irrationally or unfairly; nor was NSI granted this power only to enrich itself. At a minimum, NSI, and all other entities that have been granted privileged positions over the functioning of the Internet, must be required to act in a reasonable manner for the benefit of the Internet community.

B. In a Modern Society, Certain Critical Organizations Have a Duty to Act for the Public Good

California law has long recognized that, even in a capitalist democracy, enterprises with near monopolistic powers owe duties to the larger public because they affect the larger public. In that regard, the California Supreme Court has repeatedly held that organizations that gain near monopoly power, such that their conduct disproportionately affects the marketplace, gain along with that power a responsibility to act reasonably and serve the public good.

[M]onopoly raises duties which may be enforced against the possessors of the monopoly. This has been recognized from the earliest times. . . . [T]he holders of the monopoly must not exercise their power in an arbitrary, unreasonable manner so as to bring injury to others. The nature of the monopoly determines the nature of the duty.

James v. Marinship Corp., 25 Cal. 2d 721, 732 (1945) (quotations omitted).

In *Marinship*, the California Supreme Court held that a labor union that had gained monopolistic powers through a “closed shop” could not arbitrarily refuse membership in the union and was liable to the excluded worker if it did so. *Id.* at 740. Although the immediate beneficiaries of *Marinship* were African-American workers, the case is not a civil rights case. As subsequent case law has elaborated, near monopolistic power in any entity creates a public interest that must be protected.

Thus, in *Pinsker v. Pacific Coast Soc’y of Orthodontists*, 1 Cal. 3d 160 (1969), the court held that orthodontists could not be arbitrarily excluded from a professional organization because that organization’s monopolistic control created a public interest in the organization’s conduct.

Public policy strongly dictates that this power (of exclusion) should not be unbridled but should be viewed judiciously as a fiduciary power to be exercised in a reasonable and lawful manner for the advancement of the interests of the medical profession and the public generally.

Id. at 165. As the court later explained, the critical factor is the association’s power: “the associations still wielded monopoly power and affected sufficiently significant economic and professional concerns so as to clothe the societies with a ‘public interest.’” *Pinsker v. Pacific Coast Soc’y of Orthodontists*, 12 Cal. 3d 541, 552 (1974) (*Pinsker II*); *see also Ezekial v. Winkley*, 20 Cal. 3d 267, 272 (1977) (“The underlying rationale of the *Marinship-Pinsker* line of cases is that certain private entities possess substantial power either to thwart an individual’s pursuit of a lawful trade or profession, or to control the terms and conditions under which it is practiced.”).

The principle of these cases is not limited to membership in an organization. As the California Supreme Court stated last year, the role certain companies play in society renders them quasi-public entities subject to oversight by the courts.

Certain institutions and enterprises are viewed by the courts as quasi-public in nature: The important products or services which those enterprises provide, their express or implied representations to the public concerning their products and services, their superior bargaining power, legislative recognition of their public aspect, or a combination of these factors, lead courts to impose on these enterprises obligations to the public and the individuals with whom they deal, reflecting the role which they have assumed, apart from and in some cases despite the existence of a contract.

Potvin v. Metropolitan Life Ins. Co., 22 Cal. 4th 1060, 1070 (2000) (quoting Justice Matthew O. Tobriner & Joseph R. Grodin, *The Individual and the Public Service Enterprise in the New Industrial State*, 55 Cal. L. Rev. 1247, 1253 (1967)).

The control that NSI and similar entities wield over the Internet through their control of the DNS and related protocols is as substantial, if not more so, than the monopolistic practices at issue in the *Marinship-Pinsker-Ezekial* line of cases. The rights to speech and association provided by the Internet are just as fundamental, if not more so, than the right to work. As discussed above, because they currently have physical control over the DNS, entities like NSI literally control Internet access for every website and every country in the world. NSI controls most of these by itself through Root Server A. Under the principles of *Pinsker* and its progeny, such widespread control over a global public resource creates an equally widespread duty to act reasonably and protect the interest of domain name registrants and the Internet public at large.

VI. Conclusion

The Domain Name System is critical to the proper functioning of the Internet. If the DNS is manipulated, mismanaged or neglected, domain name registrants will be unable to maintain their domains, Internet users will be unable to find the websites they are seeking, website hosts will be unable to publish their information, ideas, and art to the Web and all publishers will be unable to convey their speech to others through e-mail or other Internet communication tools. These critical human rights to speech and association must not be held hostage to the interests, negligence or even the whim, of any corporation. They must be managed by an entity that is responsible for their proper management for the benefit of the human race and accountable for its performance of that responsibility. The district court's decision to immunize NSI from such accountability is inherently inconsistent with these principles. EFF therefore urges this Court to reverse the district court's grant of summary judgment in favor of NSI.

Dated: January __, 2002

By _____
Robin Gross, Esq.
ELECTRONIC FRONTIER FOUNDATION
Amicus Curiae

TABLE OF CONTENTS

I.	Statement of Interest	2
II.	Summary of Argument	2
III.	The Internet Benefits All of the World’s Citizens	4
IV.	Network Solutions and Other Internet Infrastructure Entities Have Been Given Substantial Technological Power Over the Internet	6
	A. The Current “Architecture” of the Internet Is Based on a Small Number of Key Infrastructure Entities.....	6
	B. As the “.Com” Registry and Custodian of Root Server A, NSI Has Been Given Unparalleled Control Over the Internet	7
V.	With Great Power Comes Great Responsibility.....	11
	A. NSI, Like All Internet Infrastructure Entities Must Act Responsibly So That the Internet Will Function Fairly and Reasonably	11
	B. In a Modern Society, Certain Critical Organizations Have a Duty to Act for the Public Good	12
VI.	Conclusion	15

TABLE OF AUTHORITIES

Cases

<i>ACLU v. Reno</i> , 929 F. Supp. 824 (E.D. Pa. 1996).....	5
<i>Ezekial v. Winkley</i> , 20 Cal. 3d 267 (1977).....	14
<i>James v. Marinship Corp.</i> , 25 Cal. 2d 721 (1945).....	12
<i>Kremen v. Cohen</i> , 99 F. Supp. 2d 1168 (N.D. Cal. 2000).....	8
<i>Pinsker v. Pacific Coast Soc’y of Orthodontists</i> , 12 Cal. 3d 541 (1974).....	13
<i>Pinsker v. Pacific Coast Soc’y of Orthodontists</i> , 1 Cal. 3d 160 (1969).....	13
<i>Potvin v. Metropolitan Life Ins. Co.</i> , 22 Cal. 4th 1060 (2000).....	14
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	2, 3, 4, 5

Other Authorities

Eugene Volokh, <i>Cheap Speech and What It Will Do</i> , 104 Yale L.J. 1805, 1833-43 (1995).....	5
Justice Matthew O. Tobriner & Joseph R. Grodin, <i>The Individual and the Public Service Enterprise in the New Industrial State</i> , 55 Cal. L. Rev. 1247, 1253 (1967).....	14

PROOF OF SERVICE

I certify that an original and fifteen (15) copies of this brief were delivered by hand to the Clerk of the United States Court of Appeals for the Ninth Circuit, 95 Seventh Street, San Francisco, California 94110, and two (2) copies were sent, via United States mail, postage pre-paid to:

James M. Wagstaffe, Esq.
Kerr & Wagstaffe LLP
100 Spear Street, Suite 1800
San Francisco, CA 94105
Attorneys for Plaintiff-Appellee/Cross-Appellant GARY KREMEN

Robert Dorband, Esq.
Duboff & Ross LLC
Hampton Oaks, Second Floor
6665 Southwest Hampton Street
Portland, OR 97223

Attorneys for Defendants/Appellants STEPHEN MICHAEL COHEN, OCEAN FUND INTERNACIONAL, LTD., YNATA LTD., and SAND MAN INTERNACIONAL LIMITED, S.A. de C.V.

Michael Mayock, Esq.
Law Offices of Michael Mayock
35 South Raymond Avenue
Pasadena, CA 91105

David H. Dolkas, Esq.
Gray Cary Ware & Freidenrich
400 Hamilton Avenue
Palo Alto, CA 94301

Attorneys for Defendant/Cross-Appellee NETWORK SOLUTIONS, INC.

Kathryn E. Karcher, Esq.
Gray Cary Ware & Freidenrich
401 B Street, Suite 2000
San Diego, CA 92101-4240

Richard S. Diestel, Esq.
Bledsoe, Cathcart, Diestel & Pedersen, LLP
601 California Street, 16th Floor
San Francisco, CA 94108-2805

The Hon. James Ware
United States District Court
280 South 1st Street
San Jose, CA 95113

Dated: January __, 2002

Robin Gross, Esq.
ELECTRONIC FRONTIER FOUNDATION
Amicus Curiae