

FOR EDUCATIONAL USE ONLY

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

121 F.Supp.2d 156

(Cite as: 121 F.Supp.2d 156)

United States District Court,
D. New Hampshire.

NATIONAL A-1 ADVERTISING, INC. and Lynn Haberstroh, Plaintiffs,
v.
NETWORK SOLUTIONS, INC., National Science Foundation, David Graves, James P. Rutt, and John/Jane Doe, Defendants.

No. CIV. 99-033-M.

Sept. 28, 2000.

Applicants for registrant of Internet domain names sued registrar, seeking injunctive and declaratory relief after registrar refused to approve names it deemed vulgar. Registrar moved for summary judgment. The District Court, McAuliffe, J., held that: (1) registrar was not public actor, capable of violating First Amendment rights of applicants, by virtue of having undertaken registration function pursuant to contract with federal government, and (2) in any event, second-level portion of Internet address was not public forum of any type, for First Amendment purposes.

Judgment for registrar.

West Headnotes

[1] Constitutional Law k82(5)

92k82(5)

A private entity will be deemed a "state actor," whose conduct may violate First Amendment, if (1) it assumes a traditional public function when it undertakes to perform the challenged conduct, or (2) an elaborate financial or regulatory nexus ties the challenged conduct to the State, or (3) a symbiotic relationship exists between the private entity and the State. U.S.C.A. Const.Amend. 1.

[2] Constitutional Law k90.4(3)

92k90.4(3)

Private contractor retained by federal government to assume responsibility for approving second-level domain names for Internet websites did not become state actor capable of violating First Amendment free speech rights of rejected applicants denied registration of allegedly vulgar names, on grounds that contractor was assuming traditional public function; it was fortuitous that federal government happened to start Internet registration process, which was not inherently governmental in nature. U.S.C.A. Const.Amend. 1.

[3] Constitutional Law k90.4(3)

92k90.4(3)

Private contractor retained by federal government to assume responsibility for approving second-level domain names for Internet websites did not become state actor capable of violating First Amendment free speech rights of rejected applicants denied registration of allegedly vulgar names, on grounds that government had imposed regulatory framework which contractor was implementing; policy of rejecting vulgar names was conceived and applied entirely by contractor, with no government approval or input. U.S.C.A. Const.Amend. 1.

[4] Constitutional Law k90.4(3)

92k90.4(3)

For purpose of determining whether contractor assuming responsibility for registering second-level Internet domain names, under contract with federal government, was state actor capable of violating First Amendment free speech rights of registration applicants through policy of rejecting proposed names it considered vulgar, evidence that the government retained right to create new top-level Internet domain names, designating classes of websites such as educational and commercial, did not reflect retention of any control over registration of second-level names. U.S.C.A. Const.Amend. 1.

[5] Constitutional Law k90.4(3)

92k90.4(3)

Private contractor retained by federal government to assume responsibility for approving second-level domain names for Internet websites did not become state actor capable of violating First Amendment free speech rights of rejected applicants denied registration of allegedly vulgar names, on grounds that symbiotic relationship existed between government and contractor; while contract in question was one of cooperation, rather than one involving a grant, record was insufficient to show that government was joint participant in ongoing registration process. U.S.C.A. Const.Amend. 1.

[6] Constitutional Law k90.1(4)

92k90.1(4)

To enforce a content-based exclusion of speech from a traditional public forum, the state must show that its regulation is necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end. U.S.C.A. Const.Amend. 1.

[7] Constitutional Law k90.1(4)

92k90.1(4)

A state may enforce content neutral time, place, and manner restrictions on speech in traditional public fora, provided those restrictions are narrowly tailored to serve a significant governmental interest and leave open ample alternative channels of communication. U.S.C.A. Const.Amend. 1.

[8] Constitutional Law k90.1(4)

92k90.1(4)

Government cannot restrict speech in designated public fora absent a compelling governmental interest. U.S.C.A. Const.Amend. 1.

[9] Constitutional Law k90.1(4)

92k90.1(4)

Permits.

When non-public forum is involved, government may either impose time, place, and manner regulations on speech within forum, or may reserve forum for its intended purposes, communicative or otherwise, as long as regulation on speech is reasonable and not an effort to suppress expression merely because public officials oppose speaker's view. U.S.C.A. Const.Amend. 1.

[10] Constitutional Law k90.4(3)

92k90.4(3)

[10] Telecommunications k461.15

372k461.15

Portion of Internet address containing second-level domain name was not a discrete forum for speech, precluding claim that entity responsible for registering proposed domain names violated First Amendment rights of applicants denied registration on grounds that proposed names were vulgar; purpose of second-level domain names was identification rather than speech, it was possible for applicant to include allegedly vulgar material into other parts of total Internet address, for whatever communicative value it might have, and once Internet user arrived at address, entire website would be displayed, with no restrictions imposed on its content. U.S.C.A. Const.Amend. 1.

***158** Jonathan S. Springer, Shaines & McEachern PA, Portsmouth, NH, Scott F. Johnson, Stein Volinsky & Callaghan, Concord, NH, Charles H. Helein, Helein & Associates, P.C., McLean, VA, for Plaintiffs.

William D. Pandolph, Sulloway & Hollis, Concord, NH, Philip L. Sbarbaro, Hanson & Molloy, Richard Phillips, Jr., U.S. Department of Justice Civil Division, Washington, DC, for Defendants.

ORDER

McAULIFFE, District Judge.

This suit arises out of Network Solutions' refusal to register approximately 30 proposed second-level Internet domain names requested by plaintiffs Lynn Haberstroh and National A-1 Advertising, Inc. ("National"), the least colorful of which are probably "tits.com" and "feelmytits.com". The remaining second-level domain names requested by Haberstroh and National are decidedly more colorful sexually-oriented words and phrases that many might find particularly vulgar and offensive. Each involves rather imaginative word combinations and includes, in some form, one or more of the words that Network Solutions deemed inappropriate

for use in second-level domain names. It is sufficient for purposes of this litigation to refer to them simply as the "Disapproved Names."

After their applications for various proposed second-level domain names were rejected, plaintiffs brought this action against Network Solutions, Inc., the National Science Foundation (the "NSF"), and various individual employees of Network Solutions, seeking declaratory and injunctive relief. Specifically, both Haberstroh and National seek a declaration that defendants' refusal to register the Disapproved Names, as second-level domain names, violated their constitutional right to freedom of speech. Additionally, National seeks compensatory and punitive damages against the individually named defendants under a *Bivens* theory. *See Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971).

Pending before the court are the following dispositive motions: Network Solutions' motion for summary judgment (document no. 19); the NSF's motion for summary judgment (document no. 51); Network Solutions' motion to dismiss National's amended complaint (document no. *159 56); and Haberstroh's motion for summary judgment (document no. 216).

Background

I. The Government's Role in the Evolution of the Internet.

To understand the issues raised in context, some review of the current operation and history of the Internet is required. The Internet is essentially a network of computer networks. It grew out of work conducted by two relatively small groups of research-oriented governmental, academic, and corporate entities. The first group was engaged in networking research and it developed and used what was known as the ARPANET. That group received its primary support from the Department of Defense and defense-related agencies. The second group, which developed and used a network of computers known as the NSFNET, consisted of many of the same entities that were included in the ARPANET, along with other entities engaged in general scientific research. It received its primary support from sources that included the NSF, other federal agencies, academic institutions, and private corporations. *See* Exhibit B to Network Solutions' motion for summary judgment, Affidavit of George Strawn, the Advanced Networking Infrastructure and Research Division Director for the Computer and Information Science and Engineering Directorate of the NSF, at para. 5.

In order for the Internet to function, each entity connected to it (e.g., computer, router, network, etc.) must have a unique numeric "address." A unique identifier is required to enable one connected computer or network to identify and send information to another connected computer or network. Those unique addresses are known as Internet Protocol Addresses or "IP addresses." *Id.*, at para 11. Initially, IP addresses were assigned, and the master address list was maintained, by one person, to insure both uniqueness and reliability. *Id.*, at para. 12. That person was Dr. Jon Postel, of the University of Southern California's Information Sciences Institute. Dr. Postel performed this service as part of his work on the ARPANET project. *Id.* Later, Dr. Postel's project became known as the Internet Assigned Numbers Authority, which administered allocation of IP addresses until November of 1998, when the Internet Corporation for Assigned Names and Numbers ("ICANN"), a private, non-profit corporation was formed and designated as the governing body responsible for IP address allocation.

IP addresses function much like Social Security numbers or telephone numbers: each IP address is unique and corresponds to a specific entity connected to the Internet. Because number strings can be cumbersome and difficult to remember, the Domain Name System ("DNS") was developed to allow users to link a unique (and easier to remember) domain name with a numeric (and more difficult to remember) IP address, thereby making it more convenient for users to access particular addresses on the Internet. So, for example, a user wishing to access the website maintained by International Business Machines need only remember the domain name "IBM.com," rather than the elaborate numerical IP address of the computer on which information relating to IBM's website is maintained (for example, a typical IP address might be something like: 192.168.0.10).

There is, however, no requirement that a person wishing to establish a website on the Internet obtain a second-level domain name. He or she can successfully operate a website after having obtained only an IP address; a second-level domain name is employed merely as a convenient access tool for other users. *See, e.g., PGMedia, Inc. v. Network Solutions, Inc.*, 51 F.Supp.2d 389, 408 (S.D.N.Y.1999), ("[T]here does not appear to be a requirement that a computer user wishing to establish an Internet site have a domain name at all. This is because domain names serve the sole purpose of making it *160 easier for users to navigate the Internet; the real networking is done through the IP numbers."), *aff'd sub nom. Name .Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573 (2d Cir.2000). In other words, the advent of domain names did not eliminate the functional necessity of IP addresses. A second-level domain name is nothing more than a more convenient way for humans to navigate to the appropriate IP address of a particular entity connected to the Internet.

Within the DNS, the domain name space is constructed as a hierarchy. It is divided into top-level domains (TLDs), with each TLD then divided into second-level domains (SLDs), and so on. Approximately 240 national, or country-code, TLDs (ccTLDs) are administered by their corresponding governments or by private groups under contracts with those governmental entities. For example, the ccTLD for Great Britain is ".uk" and the ccTLD for the United States is ".us". A small set of TLDs, known as "generic" top-level domains or gTLDs, do not carry any national identifier. Instead, they denote the intended function of that portion of the domain space. So, for example, the ".com" gTLD was established for commercial users, ".org" for not-for-profit organizations, and ".net" for network service providers.

In July of 1997, as part of the Clinton Administration's Framework for Global Electronic Commerce, the President directed the Secretary of Commerce to privatize the administration of the Domain Name System, so as to increase competition and international participation in its management and development. Accordingly, the Department of Commerce issued a Request for Comments on DNS administration, including the creation of new top-level domains and development of policies for second-level domain name registration. After considering the more than 430 comments that were received, the National Telecommunications and Information Administration ("NTIA"), an agency of the Department of Commerce, issued a policy statement entitled "A Proposal to Improve the Technical Management of Internet Names and Addresses." The proposed rule-making, or "Green Paper," was published in the Federal Register and solicited public comment. Among other things, the Green Paper proposed certain actions designed to minimize the government's involvement in overseeing aspects of Internet maintenance and increase privatization of the management of Internet names and address.

In June of 1998, NTIA published *Management of Internet Names and Addresses*, 63 Fed.Reg. 31741 (June 10, 1998) (the "NTIA Policy Statement"), which, among other things, provided a general description of the evolution of the Internet, the role that the federal government and Network Solutions have played in that development, and proposed changes to those roles:

More than 25 years ago, the U.S. Government began funding research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency (DARPA) in the 1960s. ARPANET was later linked to other networks established by other government agencies, universities and research facilities. During the 1970s, DARPA also funded the development of a "network of networks;" this became known as the Internet, and the protocols that allowed the networks to intercommunicate became known as Internet protocols (IP).

As part of the ARPANET development work contracted to the University of California at Los Angeles (UCLA), Dr. Jon Postel, then a graduate student at the university, undertook the maintenance of a list of host names and addresses

After Dr. Postel moved from UCLA to the Information Sciences Institute (ISI) at the University of Southern California *161 (U.S.C.), he continued to maintain the list of assigned Internet numbers and names under contracts with DARPA. SRI International continued to publish the lists. As the lists grew, DARPA permitted Dr. Postel to delegate additional administrative aspects of the list maintenance to SRI, under continuing technical oversight. Dr. Postel, under the DARPA contracts, also published a list of technical parameters that had been assigned for use by protocol developers. Eventually these functions collectively became known as the Internet Assigned Numbers Authority (IANA).

Until the early 1980s, the Internet was managed by DARPA, and used primarily for research purposes. Nonetheless, the task of maintaining the name list became onerous, and the Domain Name System (DNS) was developed to improve the process. Dr. Postel and SRI participated in DARPA's development and establishment of the technology and practices used by the DNS. By 1990, ARPANET was completely phased out.

The National Science Foundation (NSF) has statutory authority for supporting and strengthening basic scientific research, engineering, and educational activities in the United States, including the maintenance of computer networks to connect research and educational institutions. Beginning in 1987, IBM, MCI and Merit developed NSFNET, a national high-speed network based on Internet protocols, under an award from NSF. NSFNET, the largest of the governmental networks, provided a "backbone" to connect other networks serving more than 4,000 research and educational institutions throughout the country. The National Aeronautics and Space Administration (NASA) and the U.S. Department of Energy also contributed backbone facilities.

In 1991-92, NSF assumed responsibility for coordinating and funding the management of the non-military portion of the Internet infrastructure. NSF solicited competitive proposals to provide a variety of infrastructure services, including domain name registration services. On December 31, 1992, NSF entered into a cooperative agreement with Network Solutions, Inc. (NSI) for some of these services, including the domain name registration services. Since that time, NSI has managed key registration, coordination, and maintenance functions of the Internet domain name system. NSI registers domain names in the generic top level domains (gTLDs) on a first come, first served basis and also maintains a directory linking domain names with the IP numbers of domain name servers. NSI also currently maintains the authoritative database of Internet registrations.

In 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET. This facilitated connections between NSFNET and newly forming commercial network service providers, paving the way for today's Internet. Thus, the U.S. Government has played a pivotal role in creating the Internet as we know it today.

Id., at 31741-42. The NTIA Policy Statement describes the substantial role the federal government has played in the development of the Internet and the various policies that apply to the assignment of IP addresses and domain names.

II. *The Cooperative Agreement and Network Solutions' Authority.*

When plaintiffs attempted to register the Disapproved Names, Network Solutions was the sole registrar for new second-level domain names under the ".com", ".org", ".net", and ".edu" gTLDs. It has performed that function since 1992, pursuant to Cooperative Agreement No. NCR-9218742 (the "Cooperative Agreement"). The NSF awarded Network Solutions the Cooperative Agreement following a competitive process, pursuant to the National Science Foundation Act, 42 U.S.C. §§ 1861 et seq., and the Federal Grant and Cooperative *162 Agreement Act, 31 U.S.C. §§ 6301 et seq.

In one of his affidavits, George Strawn describes the events surrounding the formation of the Cooperative Agreement between the NSF and Network Solutions as follows:

During the early Internet, the [Internet Assigned Numbers Authority or "IANA"] had responsibility for registration of first and second-level domain names. As such, the responsibility for assigning IP numbers and registering domain names was centralized with the IANA. The Defense Information Systems Agency Network Information Center, a military contractor-operated facility, actually performed the number assignment registrations.

By the late 1980s, however, a significant number of new registrants were research and educational institutions (primarily in the .edu TLD), which were likely to be supported by NSF and other civilian research agencies. Accordingly, NSF assumed support of registration services for the non-military Internet.

Between 1987 and 1991, domain name and number registration were the responsibility of the IANA under a Department of Defense contract. The registry function was performed up to 1990 by SRI (formerly known as the "Stanford Research Institute"), and from 1991 to 1992 by Government Systems Incorporated ("GSI"). In March 1991, defendant Network Solutions, Inc. ("NSI") began to perform the registry functions as a subcontractor to GSI in support of the Defense Data Network and Internet under contract with the Defense Information Systems Agency.

In March 1992, NSF released Program Solicitation 92-24 (the "Solicitation") inviting competitive proposals for "Network Information Services Managers (NIS Managers) for NSFNET and the NREN." ... Pursuant to the Solicitation, the NIS manager responsible for non-military registration services would provide registration services for non-military domain names.

The Solicitation sought three types of "Information Services": registration services for the non-military Internet; a central directory and database service (also serving the broad Internet community); and information service (help desk, etc.) to support new institutions coming on to the Internet (usually with NSF support).

Exhibit F to Network Solutions' motion for summary judgment, Affidavit of George Strawn, at paras. 27-31.

Network Solutions submitted the best proposal in the Registration Services area, while two other entities submitted the best proposals in the remaining two areas. In the end, the three firms joined to operate under a single name: Internet Network Information Center. In December of 1992, the NSF entered into the Cooperative Agreement with Network Solutions, pursuant to which Network Solutions was designated as registrar of second-level domain names within the ".com", ".net", ".edu", and ".org" TLDs. [FN1]

FN1. The General Services Administration ("GSA") provides second-level domain name registration services in the ".gov" TLD. The Boeing Company, under a contract with the Defense Information Systems Agency, provides second-level domain name registration services in the ".mil" TLD. The Internet Assigned Numbers Authority, under a contract with the Defense Advanced Research Projects Agency, provides second-level domain name registration services in the ".int" TLD. *See* Affidavit of David Graves (Exhibit E to Network Solutions' motion for summary judgment), at paras. 17-19.

In September of 1998, the NSF transferred responsibility for administering the Cooperative Agreement to the Department of Commerce. On October 6, 1998, Network Solutions and the Department of Commerce extended the Cooperative Agreement to September 30, 2000. In November of 1998, in response to President Clinton's initiative to increase competition and promote international participation in *163 the Domain Name System, the Department of Commerce designated the Internet Corporation for Assigned Names and Numbers ("ICANN") as the body responsible for DNS policy. As such, ICANN assumed responsibility for performing those functions that had been performed by the IANA and other entities, such as establishing DNS policy, IP address space allocation, protocol number parameter assignments, and root server system management functions. *See* Exhibit B to Network Solutions' motion for summary judgment, Affidavit of George Strawn, at para. 31.

In the Spring of 1999, ICANN authorized five entities to compete with Network Solutions in the registration of second-level domain names. *Id.*, at para. 32. Subsequently, additional entities were authorized to perform domain name registration services. [FN2] Thus, Network Solutions is no longer the sole registrar of proposed second-level domain names. Nor does Network Solutions have the authority to preclude the registration of second-level domain names by any of the other entities currently acting as registrars, at least some of which appear perfectly willing to register virtually any proposed second-level domain name (as long as the proposed name complies with technical protocols like, for example, the requirement that it not exceed 63 characters).

FN2. Currently, there are more than 60 organizations worldwide operating as domain name registrars in the .com, .net, and .org TLDs. *See ICANN List of Accredited and Accreditation-Qualified Registrars* (visited Sept. 13, 2000) <<http://www.icann.org/registrars/accredited-list.html>>.

III. *Navigating the Internet.*

Finally, it is, perhaps, appropriate to briefly consider how a user actually navigates the Internet and accesses various materials available on the Internet. The Internet itself is a global network of networks--the "information superhighway." It includes numerous fora through which users can disseminate information, engage in discussions, or post opinions, including, for example,

USENET newsgroups, mail exploders (also known as "listservs"), and chat rooms. Perhaps the most well-known method of communicating information across the Internet is the Worldwide Web or simply the "Web."

Many laypeople erroneously believe that the Internet is co-extensive with the Web. The Web is really a publishing forum; it is comprised of millions of separate "Web sites" that display content provided by particular persons or organizations. Any Internet user anywhere in the world with the proper software can create a Web page, view Web pages posted by others, and then read text, look at images and video, and listen to sounds posted at these sites.

American Libraries Ass'n v. Pataki, 969 F.Supp. 160, 166 (S.D.N.Y.1997).

Information is published on the Web using a formatting language known as Hypertext Markup Language or HTML. A computer user who wishes to access resources on the Web utilizes a Web "browser," such as the now generally familiar Netscape Navigator or Internet Explorer. A browser is software that can display HTML documents containing text, images, sound, and moving video. By employing a Web browser, users can access particular sites on the Web in several ways. First, they can simply type the address of a desired site directly into the address bar on their browser. That address, which is known as the Universal Resource Locator or "URL," includes, as one of its technical components, the second-level domain name. Armed with that second-level domain name, the browser software then contacts a remote computer, known as a Domain Name Server. The Domain Name Server translates the requested second-level domain name into the assigned unique IP address associated with the name. Having acquired the appropriate numeric IP address, the browser then contacts *164 the server located at that address, which in turn sends a copy of the text and any graphics associated with that particular Web page back to the browser for display on the user's monitor.

Alternatively, a person can use his or her computer mouse to click on a "hyperlink" to a website and be connected directly to that site.

Any HTML document can include links to other types of information or resources, so that while viewing an HTML document that, for example, describes resources available on the Internet, an individual can "click" using a computer mouse on the description of the resource and be immediately connected to the resource itself. Such "hyperlinks" allow information to be accessed and organized in very flexible ways, and allow individuals to locate and efficiently view related information even if the information is stored on numerous computers all around the world.

American Civil Liberties Union v. Reno, 31 F.Supp.2d 473, 483 (E.D.Pa.1999), *aff'd*, 217 F.3d 162 (3rd Cir.2000). When a user clicks on a hyperlink, his or her browser software is automatically provided with the URL of the linked or target website. Accordingly, that URL then appears in the browser's address bar and the process of converting the second-level domain name into an IP address described above is repeated. Once the IP address is resolved, the browser contacts the server located at that address, obtains the particular page that the user seeks, and displays the contents of that page on the user's computer monitor.

Finally, a user might employ a "search engine" such as Yahoo!, Alta Vista, or Northern Light. Search engines are databases that list most sites accessible on the Web. The user simply types a key word or words as a "search" request and the search engine then returns a list (usually in the form of hyperlinks) of various sites that contain one or more of the search terms. In order to increase the likelihood that their pages will be returned as a "hit" by the various search engines,

Web page designers embed key words in their Web Pages, known as "meta-tags." Although normally invisible to the Internet user, meta-tags are detected by search engines and increase the likelihood that a user searching for a particular topic will be directed to that Web designer's page.

So, for example, the homepage of General Motors' website contains the following meta-tags: "General Motors, GM, Buick, Cadillac, Chevrolet, EV1, GMC, Holden, Isuzu, Oldsmobile, Opel, Pontiac, Saab, Saturn, Vauxhall, Detroit, Car, Cars, Truck, Trucks, Driver, Drivers, Driving, Driving experience, Innovations, Vehicle, Vehicles, Automobile, Automobiles, Automotive." General Motors Home Page (visited September 13, 2000) <<http://www.GM.com>>. By embedding those "invisible" meta-tags in its home page, General Motors increases the likelihood that a user employing a search engine to locate websites containing information on General Motors' products (or automotive products in general) will be directed to the GM website.

Discussion

I. Plaintiffs' Efforts to Register Domain Names.

In 1996 (while it was still the exclusive registrar of second-level domain names), Network Solutions apparently adopted a policy under which it declined to register second-level domain names that contained six of the seven words prohibited for broadcast by the FCC and major television networks (the seven "Filthy Words" made famous by comedian George Carlin). *See Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726, 98 S.Ct. 3026, 57 L.Ed.2d 1073 (1978). The seventh "filthy" word, with regard to which Network Solutions will grant second-level domain name registrations, relates to the character string s-h-i-t. Due to the prevalence of that character string in what Network Solutions considers "otherwise *165 legitimate" words (for example, a large percentage of Japanese commercial names and surnames, such as "Matsushita" and "Yamashita") Network Solutions decided that it would accept registrations for domain names that included that string of characters. Importantly, however (at least for "state action" purposes, discussed below), Network Solutions says the decision to implement a decency policy was entirely its own, asserting that the NSF "did not direct, decide, approve, or in any other way require Network Solutions' adoption of its [decency policy]." Exhibit D to Network Solutions' motion for summary judgment, Affidavit of David Graves, Director of Business Affairs for Network Solutions, at para. 12.

As of May, 1999, Network Solutions was registering second-level domain names at the rate of over 300,000 per month, or a new domain name approximately every 10 seconds. *Id.*, at para. 9. Not surprisingly, that registration process is entirely automated and Network Solutions' practice of rejecting proposed domain names containing any of the six restricted character strings is triggered automatically, by filtering software. That filter blocks the registration of second-level domain names, such as those submitted by plaintiffs, that contain the exact letter strings contained in the six restricted words (e.g., "tits" is one of the restricted character strings and, therefore, "feelmytits.com"--one of the domain names that National sought to register--was filtered and rejected).

National says Network Solutions rejected approximately 22 of its applications for second-level domain names, each time concluding that the proposed name was "inappropriate" under its decency policy. Haberstroh claims that Network Solutions rejected six of her applications for domain names under that policy. As noted above, the only domain name as to which both

plaintiffs claim an interest is "tits.com".

After Haberstroh filed her complaint, Network Solutions transferred the registration of four of the six domain names Haberstroh sought to register (the "Protected Names") from the United States District Court for the Middle District of California to this court, to insure that they would not be registered to other applicants (by other domain name registrars) while this action was pending. It appears, however, that "tits.com" and one of the other second-level domain names sought by Haberstroh had already been registered to a third party by another registrar.

On July 16, 1999, through Net Wizards, Inc., one of the other registrars now competing with Network Solutions in the registration of domain names, National successfully registered four of the second-level domain names originally rejected by Network Solutions. *See* National's amended complaint (document no. 46), at para. 50. However, it appears that, as of that date, the remaining names that National originally sought to register through Network Solutions had already been registered to other users. *Id.*, at para. 51. Because each second-level domain name must be unique, neither Haberstroh nor National can obtain those that have been registered to third parties, even if the court were to order Network Solutions to accept their applications or even if plaintiffs were to attempt to register those names through another registrar, such as Net Wizards. If plaintiffs want those domain names, it would appear that they must negotiate their purchase from those who currently own them or wait and hope that those names are not renewed by their current owners.

II. *Network Solutions' Motion for Summary Judgment.*

A. *State Action.*

The core of plaintiffs' complaint is that Network Solutions violated their First Amendment rights. The First Amendment provides that "Congress shall make no law ... abridging the freedom of speech." U.S. Const. amend. I. By its very terms, the Amendment proscribes *166 governmental conduct, not conduct undertaken by private citizens. *See Public Utilities Commission of District of Columbia v. Pollak*, 343 U.S. 451, 461, 72 S.Ct. 813, 96 L.Ed. 1068 (1952) (holding that the First Amendment applies "to and restrict[s] only the Federal Government and not private persons."). *See also Massachusetts Universalist Convention v. Hildreth & Rogers Co.*, 183 F.2d 497, 501 (1st Cir.1950) (holding that the First Amendment "limits only the action of Congress or of agencies of the federal government and not private corporations such as defendant here."). Accordingly, if Network Solutions was not a state actor when it acted as registrar for second-level domain names, the First Amendment did not restrict it from imposing limits on the words or phrases that it would accept for registration. In fact, the First Amendment guarantees private actors the right not to be associated with speech with which they disagree. *See, e.g., Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557, 115 S.Ct. 2338, 132 L.Ed.2d 487 (1995). [FN3]

FN3. During the period of time relevant to this case, Network Solutions was the sole registrar of second-level domain names. Consequently, any informed person encountering an offensive or objectionable second-level domain name would know that it was registered by Network Solutions.

[1] Consequently, a fundamental issue raised by plaintiffs' complaint is whether Network Solutions was acting as an arm or agent of the federal government when it rejected plaintiffs' proposed second-level domain names. Stated somewhat differently, the question is whether Network Solutions' decision not to register the Disapproved Names constitutes "state action," a term that includes conduct taken under color of federal law. *See Dobyys v. E-Systems, Inc.*, 667 F.2d 1219, 1220 n. 1 (5th Cir.1982). Resolution of that issue requires application of a three-part analysis to the particularly complex facts presented in this case (i.e., the government's role in the evolution of the Internet and, in particular, the historical role the government played in establishing and controlling second-level domain name registration). *See, e.g., Perkins v. Londonderry Basketball Club*, 196 F.3d 13, 18 (1st Cir.1999) (holding that a private entity will be deemed "a state actor if (1) it assumes a traditional public function when it undertakes to perform the challenged conduct, or (2) an elaborate financial or regulatory nexus ties the challenged conduct to the State, or (3) a symbiotic relationship exists between the private entity and the State."). *See also Barrios-Velazquez v. Asociacion De Empleados*, 84 F.3d 487, 491-94 (1st Cir.1996).

1. Similar Future Litigation is Unlikely.

The government's role in the Internet is deliberately waning. By design, the private sector is assuming an ever-increasing role in determining relevant policies and protocols, and domain name registration is now a competitive endeavor, over which Network Solutions no longer holds any exclusive control. All of those factors would effectively negate an assertion that Network Solutions *currently* acts under color of state law when registering domain names.

Moreover, because at least some of the entities now providing domain name registration services appear to be perfectly willing to register virtually any proposed second-level domain name, the issues raised in this case are unlikely to present themselves in future litigation. That is to say, because applicants can now freely register second-level domain names that contain nearly any conceivable words or phrases, it is unlikely that the courts will face future controversies arising from the rejection of second-level domain names based solely on the claim that they are vulgar or offensive. Anyone interested in registering a domain name without fear of rejection need only avoid Network Solutions and process the *167 registration through Net Wizards or one of the other competing registrars.

Notwithstanding the foregoing, it is necessary to consider whether Network Solutions was a "state actor" when it denied plaintiffs' applications to register the Disapproved Names as second-level domain names.

2. The Perkins Test and State Action.

[2] Because of the relative novelty of the Internet, there is very little precedent applying traditional and familiar legal principles to its operation. But, as Network Solutions correctly notes, at least one court of appeals has concluded that the registration of domain names is not a "traditional governmental function," thereby suggesting that Network Solutions does not meet the first of the three "state action" tests identified in *Perkins* (and also implying that Network Solutions was not acting under color of state law when it rejected plaintiffs' proposed second-level domain names). *See Thomas v. Network Solutions, Inc.*, 176 F.3d 500, 511 (D.C.Cir.1999)

("A recent and novel function such as domain name registration hardly strikes us as a 'quintessential' government service."), *cert. denied*, 528 U.S. 1115, 120 S.Ct. 934, 145 L.Ed.2d 813 (2000).

Nevertheless, plaintiffs do present a plausible argument that, at least during the time period relevant to this litigation, Network Solutions was indeed performing a "traditional" government service by acting as a registrar of domain names. The Internet as it exists today is, after all, the direct descendant of two governmental creations: the ARPANET and NSFNET. Since the inception of those ancestors to the Internet, lists of networked computers' IP addresses (and eventually domain names) had to be maintained in order for the network to function. And, while the "tradition" of maintaining those lists and registering new additions to them is not a long one, it is a function over which the government has exercised substantial oversight from the Internet's inception. The federal government has, until very recently, undertaken responsibility (either directly or indirectly, through private contractors) to make certain that such registrations: (a) actually occurred; and (b) were conducted in a logical and orderly way. Thus, the court is not persuaded that the mere novelty of the Internet is sufficient to preclude a finding that the registration of second-level domain names is a traditional governmental function that was delegated to Network Solutions.

Importantly, however, the mere fact that Network Solutions was, during the period relevant to this proceeding, arguably engaged in a public function does not compel the conclusion that it was a "state actor" when performing the role of second-level domain name registrar. As the Court of Appeals for the First Circuit has observed:

The public function analysis is designed to flush out a *State's attempt to evade its responsibilities by delegating them to private entities*. See *Barrios-Velazquez*, 84 F.3d at 494. In order to prevail on such a theory, *a plaintiff must show more than the mere performance of a public function by a private entity; she must show that the function is one exclusively reserved to the State*. See *id.* at 493-94. Government customarily involves itself in many types of activities, but few of those activities come within the State's exclusive preserve. To date, the short list of activities that have been held to satisfy this demanding criterion includes "the administration of elections, the operation of a company town, eminent domain, preemptory challenges in jury selection, and, in at least limited circumstances, the operation of a municipal park." *United Auto Workers v. Gaston Festivals, Inc.*, 43 F.3d 902, 907 (4th Cir.1995) (citations omitted). When a plaintiff ventures outside such narrow confines, she has an uphill climb.

Perkins, 196 F.3d at 18-19 (emphasis supplied).

***168** Whether Network Solutions was a "state actor" when it denied plaintiffs' applications to register the Disapproved Names as second-level domain names is, to say the least, a complex question. Solid arguments can certainly be made on both sides of the issue though, in the end, the court is persuaded that Network Solutions was *not* a state actor during the period of time relevant to this litigation. First, there is no evidence that the government sought to "evade its responsibilities by delegating them to private entities," such as Network Solutions. See *Perkins*, 196 F.3d at 18-19. The government's role in developing a privately accessible Internet was clearly one of facilitation and not one of delegation of a governmental function.

[3] Nor is there any evidence that the government imposed any regulatory restrictions (amounting

to "coercion") with regard to the registration of second-level domain names. *See id.*, at 19. Because many of the competitors now registering second-level domain names freely grant applications for what some might consider vulgar or offensive domain names, one might reasonably infer that (at least presently) the government has no interest in, nor has it imposed any restriction on, what words or phrases may appear in second-level domain names. That fact, while not determinative, certainly undermines plaintiffs' apparent assertion that there were once elaborate governmentally imposed regulatory restrictions controlling Network Solutions' registration of domain names (the second of three tests for "state action" identified in *Perkins, supra*). And, perhaps more importantly, plaintiffs have failed to point to any evidence that might establish that, during the period of time relevant to this case, the government actually played a role in, or imposed any restrictions on, Network Solutions' registration of second-level domain names. *See Barrios-Velazquez*, 84 F.3d at 493 ("The test is whether the government exercised *coercive power* or provided such *significant encouragement* that the complained-of misconduct ... must be deemed to be the conduct of the government.") (emphasis supplied).

Here, the "complained-of misconduct" is plainly Network Solutions' refusal, based on its own decency policy, to register the Disapproved Names. Both the NSF and Network Solutions have submitted evidence supporting their assertion that the decision to implement the decency policy was entirely Network Solutions'; the NSF had no input into that decision and certainly appears to have had little, if any, interest in how (or even whether) Network Solutions decided which proposed second-level domain names were "appropriate" and which were not. *See, e.g.*, Exhibit A to Network Solutions' motion for summary judgment, Affidavit of David M. Graves at para. 23 ("The NSF did not direct, decide, approve, or in any way require Network Solutions' adoption of its [decency policy]."); Exhibit B to Network Solutions' motion for summary judgment, Affidavit of George Strawn at para. 28 ("NSF engaged in general oversight of [Network Solution's] performance of its responsibilities under the Agreement, but not [its] day-to-day managerial activities such as [Network Solution's] policy relating to the appropriateness of proposed second-level domain names."). *See also* Exhibit C to Network Solutions' motion for summary judgment, Affidavit of Attorney Lawrence Rudolph, General Counsel to the NSF, at para. 3 ("NSF never involved itself with [Network Solutions'] policy relating to the appropriateness of proposed second-level domain names that its customers seek to register. NSF had no input--supervisory, indirect, or otherwise--with this policy of [Network Solutions], as the appropriateness policy was not within our oversight responsibilities under the Cooperative Agreement.").

[4] Evidence that the government did exercise control over Network Solutions' ability to create new *top-level* domain names (a point repeatedly reiterated by plaintiffs) is of course irrelevant to whether *169 the government exercised a "coercive" or "encouraging" role in Network Solutions' registration of *second-level* domain names. Top level domain names serve an entirely different and distinct function and the NSF's interest in regulating precisely when and how new top-level domain names are created sheds no light whatsoever on whether it exercised any influence or control over Network Solutions' day-to-day registration of second-level domain names.

[5] Finally, notwithstanding the government's use of a cooperative agreement (rather than a federal grant) to facilitate and support Network Solutions' role as private sector second-level domain name registrar, *compare* 31 U.S.C. § 6304 *with* 31 U.S.C. § 6305, the court is not persuaded that the relationship between the government and Network Solutions can properly be viewed as "symbiotic." *See Perkins*, 196 F.3d at 21 ("In terms, this test requires an evaluation of

whether the government 'has so far insinuated itself into a position of interdependence with the private entity that it must be recognized as a joint participant in the challenged activity.' ") (citation omitted). Simply stated, there is insufficient evidence in the record to support the conclusion that the federal government was a "joint participant" in Network Solutions decision to reject the Disapproved Names. To the contrary, it is fairly apparent that the government's policy and actions are designed to extricate itself from involvement in the Internet's operations.

Consequently, applying the three-part test adopted by the court of appeals in *Perkins*, the court concludes that Network Solutions was not a government actor when it denied plaintiffs' applications for second-level domain names. Certainly there is room for disagreement on that point, but even if Network Solutions did qualify as a government actor, it did not violate plaintiffs' First Amendment rights, as explained below.

B. *The First Amendment.*

To assess the validity of plaintiffs' First Amendment claims, the court must first determine whether second-level domain names constitute or are capable of communicating speech protected by the First Amendment. If so, the next step is to identify the nature of the forum in which that speech is communicated, since that dictates the extent to which the government (here, Network Solutions) may restrict such speech. *See generally Cornelius v. NAACP Legal Defense and Educational Fund, Inc.*, 473 U.S. 788, 797, 105 S.Ct. 3439, 87 L.Ed.2d 567 (1985).

Of course, the mere fact that many might consider the Disapproved Names vulgar, crass, or personally offensive does not put those words outside the protections of the First Amendment. *See, e.g., Cohen v. California*, 403 U.S. 15, 24-25, 91 S.Ct. 1780, 29 L.Ed.2d 284 (1971) ("[w]hile the particular four-letter word being litigated here is perhaps more distasteful than most others of its genre, it is nevertheless often true that one man's vulgarity is another's lyric. Indeed, we think it is largely because governmental officials cannot make principled distinctions in this area that the Constitution leaves matters of taste and style so largely to the individual."); *Reno v. American Civil Liberties Union*, 521 U.S. 844, 874, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997) ("In evaluating the free speech rights of adults, we have made it perfectly clear that 'sexual expression which is indecent but not obscene is protected by the First Amendment.' Indeed, [this Court has previously] admonished that 'the fact that society may find speech offensive is not a sufficient reason for suppressing it.' ") (citations omitted).

1. *Domain Names and Protected Speech.*

It appears that very few courts have given focused consideration to whether second-level domain names constitute or are capable of communicating protected speech. The Court of Appeals for the *170 Second Circuit recently concluded that the existing generic *top*-level domain names (e.g., .com, .gov, .edu), all of which are limited to three letters, do not constitute protected speech. *Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d at 585. The court went on, however, to suggest in *dicta* that future top-level domain names (and, by necessary implication, second-level domain names) might well constitute protected speech:

The Internet in general, and the DNS in particular, is marked by extraordinary plasticity. The DNS has already undergone considerable change in the Internet's brief history to date, and may undergo even more radical changes in the near future under the auspices of ICANN and DNSO.

There is nothing inherent in the architecture of the Internet that prevents new gTLDs from constituting expressive speech.

* * * * *

Further, the functionality of domain names does not automatically place them beyond the reach of the First Amendment. Although domain names do have a functional purpose, whether the mix of functionality and expression is "sufficiently imbued with the elements of communication" depends on the domain name in question, the intentions of the registrant, the contents of the website, and the technical protocols that govern the DNS.

Id. (emphasis supplied). Consequently, the court concluded that, "Domain names and gTLDs per se are neither automatically entitled to nor excluded from the protections of the First Amendment, and the appropriate inquiry is one that fully addresses particular circumstances presented with respect to each domain name." *Id.*, at 586.

A few federal courts have considered whether specific second-level domain names (as distinguished from second-level domain names in general) constitute protected speech under the First Amendment. For example, in *Planned Parenthood Federation of America, Inc. v. Bucci*, 1997 WL 133313, 42 U.S.P.Q.2d 1430 (S.D.N.Y. March 24, 1997), *aff'd*, 152 F.3d 920 (2d Cir.1998) (unpublished table decision), *cert. denied*, 525 U.S. 834, 119 S.Ct. 90, 142 L.Ed.2d 71 (1998), the court concluded that the defendant's use of the domain name "plannedparenthood.com" was not communicative and, instead, served only as a "source identifier," by which the defendant directed users to his anti-abortion website. *Id.*, at *10. Consequently, the court held that "because defendant's use of the term 'planned parenthood' is not part of a communicative message, his infringement on plaintiff's mark is not protected by the First Amendment." *Id.* See also *OBH, Inc. v. Spotlight Magazine, Inc.*, 86 F.Supp.2d 176 (W.D.N.Y.2000) (holding that the defendant's use of the domain name "the buffalonews.com" was not protected speech); *Jews for Jesus v. Brodsky*, 993 F.Supp. 282, 286-87 n. 1 (D.N.J.1998) (concluding that defendant's use of the domain names "JewsForJesus.org" and "Jews-for-Jesus.com" did not implicate rights guaranteed by the First Amendment), *aff'd*, 159 F.3d 1351 (3rd Cir.1998) (unpublished table decision).

Had the defendant in *Planned Parenthood* used a domain name such as "chooselife.com" or "stopabortion.com" he might have had a stronger claim that his domain name was meant to communicate an arguably protected message or idea. See, e.g., *Bally Total Fitness Holding Corp. v. Faber*, 29 F.Supp.2d 1161 (C.D.Cal.1998) (holding that defendant's use of the phrase "Ballysucks" in his Web address--"www. compupix.com/ ballysucks"--which linked users to a Web page on which defendant commented on business practices of Bally's that he found distasteful, did constitute speech protected by the First Amendment). That a second-level domain name might itself contain arguably protected speech does not, however, resolve the issue discussed below as to whether the space occupied by second-level domain names (that is, the space immediately to the left *171 of ".com") constitutes a discrete "forum" for speech.

In this case, it is difficult to determine whether the Disapproved Names constitute protected speech under the test approved by the Second Circuit in *Name.Space*. First, because the Disapproved Names were never registered, there are no websites associated with them. Consequently, it is impossible to determine whether the content of the website to which the domain name is linked sheds some light on whether the domain name itself communicates any

message. Additionally, precisely what motivated plaintiffs' efforts to register the Disapproved Names, or what they intended to do with those domain names once registered, is unclear. They might, for example, have merely sought to obtain those names for resale to others. Alternatively, they might have intended to operate one or more websites (either commercial or private) linked to those names. That, in turn, makes it difficult to discern whether plaintiffs' "speech" should be understood as private or commercial.

In short, all the court presently has before it are the Disapproved Names themselves. And, looking only at those names, one might plausibly argue that some are expressive of some sort of message or idea, while others are not. For example, one might assert that the domain name "feelmytits.com" is invitational communicative speech. The domain name "tits.com", on the other hand, would appear to convey little in the way of any message or idea and, instead, acts simply as a "source identifier," informing potential audience members that the website associated with that name probably contains information or perhaps even photographs relevant to that subject.

To be sure, this is an interesting legal issue. However, because the court concludes that the *space* occupied by second-level domain names does not constitute a discrete "forum" for speech, it is not necessary to determine whether, in addition to acting as proposed pointers to plaintiffs' website(s), any of the Disapproved Names are also capable of or do in fact communicate protected speech.

2. Domain Names and First Amendment Fora.

[6][7][8] The Supreme Court has identified three distinct categories of fora in which speech might be communicated: the traditional public forum, the designated public forum, and the non-public forum. *See Cornelius v. NAACP Legal Defense and Educational Fund, Inc.*, 473 U.S. 788, 105 S.Ct. 3439, 87 L.Ed.2d 567 (1985); *Perry Education Ass'n v. Perry Local Educators' Ass'n.*, 460 U.S. 37, 103 S.Ct. 948, 74 L.Ed.2d 794 (1983). Traditional public fora, such as streets, sidewalks, and parks, are "places which by long tradition or by government fiat have been devoted to assembly and debate." *Perry*, 460 U.S. at 45, 103 S.Ct. 948. In these places, "to enforce a content-based exclusion [the state] must show that its regulation is necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end." *Id.* Alternatively, the state may enforce content neutral "time, place, and manner" restrictions on speech in traditional public fora, provided those restrictions are narrowly tailored to serve a significant governmental interest and leave open ample alternative channels of communication. *Id.* And, as with the traditional public fora, the government cannot restrict speech in designated public fora absent a compelling governmental interest. *See Cornelius*, 473 U.S. at 800, 105 S.Ct. 3439.

[9] The standards governing restrictions on speech in the non-public forum are, however, less stringent. *See Perry*, 460 U.S. at 46, 103 S.Ct. 948 ("Public property which is not by tradition or designation a forum for public communication is governed by different standards."). Consequently, the Court has held that "In addition to time, place, and manner regulations, the state may reserve the [non-public] *172 forum for its intended purposes, communicative or otherwise, as long as the regulation on speech is reasonable and not an effort to suppress expression merely because public officials oppose the speaker's view." *Id.*

[10] Few would deny that features of the Internet, such as the Worldwide Web, chat rooms, bulletin board services, and newsgroups, have become fora for public debate. That does not, however, compel the conclusion that *all* conceivable means of communication associated with the Internet necessarily constitute "fora" for protected speech. *See e.g., Loving v. Boren*, 956 F.Supp. 953, 955 (W.D.Okla.1997) (concluding that University of Oklahoma's "computer and Internet services do not constitute a public forum."), *aff'd*, 133 F.3d 771 (10th Cir.1998). In this case, the focus is necessarily on the space in an Internet Web address (or URL) occupied by the second-level domain name, and the issue is whether that space constitutes a "forum" for speech. So, for example, in the hypothetical Web address <http://www.feelmytits.com>, the plaintiffs assert that the space occupied by the phrase "feelmytits" is a recognized forum for public speech and debate, in which they have been denied the opportunity to engage in constitutionally protected speech.

As noted above, the primary purpose of a second-level domain name is to provide a convenient means by which an Internet user can direct his or her computer (browser) to obtain the unique numeric IP address of another entity connected to the Internet. The Domain Name System serves as a means by which to assist users in *locating* a specific Internet site; the DNS hierarchy or architecture is not designed to act nor does it function as a forum for the dissemination of ideas, discussion, or debate. Instead, such communication, speech, debate, and the dissemination of ideas and information takes place (and is generally understood to take place) on the multitude of Web pages connected to the Internet, in the various chat rooms, on the countless bulletin boards, and in the thousands of Internet newsgroups.

Plainly, then, unlike streets, sidewalks, and parks, the space occupied by second-level domain names does not constitute a traditional public forum for discussion and debate. And, in light of that space's primary purpose (which is functional, rather than communicative), and the fact that the government has taken no affirmative steps evidencing an intent to "open up" a nontraditional forum of communication to the public, the court concludes that the space occupied by second-level domain names is not a designated public forum. As the Supreme Court observed:

The government does not create a public forum by inaction or by permitting limited discourse, but only by *intentionally opening a nontraditional forum for public discourse*. Accordingly, the Court has looked to the policy and practice of the government to ascertain whether it intended to designate a place not traditionally open to assembly and debate as a public forum. The Court has also examined the *nature of the property and its compatibility with expressive activity* to discern the government's intent.

Cornelius, 473 U.S. at 802, 105 S.Ct. 3439 (citation omitted) (emphasis supplied).

Although unquestionably not intended or designed to serve as a forum for speech, a second-level domain name could be fashioned in such a way that it is capable of communicating a brief message or idea--even a highly protected political idea or message (e.g., "JonesForPresident.com"). Thus, second-level domain names might be loosely analogized to motor vehicle license plates, or telephone numbers expressed in acronym form. They are specifically designed to serve a functional (rather than communicative) role but, in certain circumstances, they can be manipulated or used to convey a brief message or express an abbreviated or pithy opinion. In the case of license plates, that message is typically limited to no more than six or seven alphanumeric*173 characters. In the case of second-level domain names, the message is limited by technical requirements to no more than 63 characters (as a practical matter, however, domain names are typically limited to far fewer characters). *See Thomas v.*

Network Solutions, 176 F.3d at 503.

One might plausibly posit that, like license plates, the space occupied by second-level domain names falls into the third category of fora: the non-public forum, "which is not by tradition or designation a forum for public communication." *Perry*, 460 U.S. at 46, 103 S.Ct. 948. With regard to license plates, as with other categories on non-public fora, a state may impose reasonable regulations on what can be displayed on so-called vanity plates, so long as those restrictions are view-point neutral. See generally *Lewis v. Wilson*, 89 F.Supp.2d 1082 (E.D.Mo.2000) (in which the plaintiff challenged the state's decision to revoke her "ARYAN-1" vanity license plate). See also *Kahn v. Dept. of Motor Vehicles*, 16 Cal.App.4th 159, 20 Cal.Rptr.2d 6 (1993) (upholding state's decision to revoke plaintiff's vanity license plate which bore the word "fuck" in stenographic shorthand). That is, the government may impose restrictions on speech in a non-public forum, provided the restrictions are both rational and viewpoint neutral.

But, notwithstanding the arguable value of the license plate analogy, the court concludes that the space occupied by second-level domain names should not be deemed a discrete "forum" at all. Simply because people might wish to fashion second-level domain names to serve the additional purpose of expressing an opinion or idea does not lead to the conclusion that second-level domain name space constitutes a "forum" for speech or debate. See *Cornelius*, 473 U.S. at 805, 105 S.Ct. 3439 ("The Government did not create the CFC for purposes of providing a forum for expressive activity. That such activity occurs in the context of the forum created does not imply that the forum thereby becomes a public forum for First Amendment purposes.").

Beyond the fact that the space occupied by second-level domain names was plainly not intended to function as a forum, it is difficult to see how that space is even capable of effectively serving as a forum for arguably protected speech. All recognized public and non-public fora share a common characteristic: they provide some means by which a speaker might disseminate his or her message to an audience. So, for example, a speaker might proclaim his or her message on a sidewalk or in a park, where anyone willing to stop and listen will hear it. Alternatively, a person might pass out leaflets bearing a written message. Similarly, billboards or radio broadcasts provide a means by which messages can be disseminated to all who see or hear them. Even vanity license plates are openly (and unavoidably) displayed to the public, and, in that way, proclaim to those who see them the owner's limited message.

Second-level domain names, however, are altogether different. Most obviously, they are visible to a computer user under only very limited circumstances. The first is when the user manually types a domain name (as part of a full URL) into the address bar on his or her Internet browser software. In that circumstance, however, the holders or owners of the domain name are not disseminating their "message" and it is difficult to see how they are engaged in any form of speech. Instead, it is the *user* who is manually typing the message or speech represented by the domain name into his or her computer. In other words, when a computer user types <http://www.tits.com> into his or her browser's address bar, the *plaintiffs* are not engaged in any form of communicative or protected speech.

Alternatively, a user might be exposed to a second-level domain name when he or she clicks on a hyperlink to the website linked to that name (and its associated IP address). At that point, the full Universal *174 Resource Locator or "URL" of the target website--including the second-level

domain name--will be displayed in the address bar on the user's browser. For example, a user might be viewing a Web page with a hyperlink to one of plaintiffs' sites. When the user clicks on that link, the URL of the target website (e.g., <http://www.tits.com>) will appear in the browser's address bar and, simultaneously, the user will be connected to that website and the contents of the page at the target location will be displayed on the user's monitor. So, at the same time plaintiffs' asserted "message" is displayed in the small address bar at the top of the user's browser, the full contents of the target Web page is displayed on the user's monitor. And, of course, plaintiffs are free to include virtually any message they desire on that Web page, *without* the intervention or approval of Network Solutions. Viewed somewhat differently, there is no need to contort the second-level domain name (with its 63 character limit) into a vehicle for speech when, at the same time, one might use the virtually unlimited space of the Web page itself.

All of this undermines plaintiffs' assertion that the space occupied by second-level domain names constitutes a "forum" for protected speech. Because the full URL of a target website (including the second-level domain name) is displayed in the address bar at the same time that the text, photographs, and or video on that page is displayed on the user's monitor, there is simply no need for someone to attempt to communicate his or her "message" in the limited space available to second-level domain names. That message can more easily and thoroughly (and simultaneously) be conveyed in a far more comprehensive way in an unrestrained forum intended and designed for that very purpose--the Web page itself.

Nevertheless, plaintiffs persist in arguing that the space occupied by second-level domain names is an independent, free-standing forum unto itself. As noted above, the only time the owner of a second-level domain name might arguably disseminate a message to the public (or be engaged in arguably protected speech) is when: (a) a computer user clicks on a hyperlink to the website associated with that domain name, at which point the website's full URL is displayed in the user's address bar; or (b) when one or more of the Web pages maintained by that person is returned as a "hit" by a search engine and the URLs for those pages are listed for the user.

At this point, it is important to note the distinction between second-level domain names and URLs. An entity's second-level domain name is just one component of its URL. The domain name (and its associated IP address) describes a specific entity, such as a server, connected to the Internet; it does *not* refer to a particular file or Web page. Instead, files or Web pages on computers connected to the Internet are identified by their URLs, which include: (a) the transfer protocol required to access the file (e.g., "http" ("Hypertext Transfer Protocol") for files created in HTML, or "ftp" ("File Transfer Protocol") for documents created using more traditional word processing formats, etc.); (b) the domain name; and (c) the path on the host computer to a particular directory and page. So, for example, the URL `<http:// www.uscourts.gov/history/ contents.html>` includes the protocol necessary to access the site ("http") and the domain name or location of the host computer on the Worldwide Web ("www.uscourts.gov"). "/History" refers to a particular directory on that computer and, finally, "/contents.html," refers to a particular file in that directory.

In advancing arguments to support their asserted First Amendment right to secure the requested Disapproved Names as second-level domain names, plaintiffs have failed to articulate why the court should focus on the discrete functional space occupied by second-level domain names as a forum for speech, to the exclusion of the *175 other space within the URL. And, the court can

discern no constitutionally mandated (or even rational) reason why its inquiry must be limited exclusively to that discrete, technical component of an Internet address. In short, nothing about the way that second-level domain names function and nothing about the way that they are employed suggests that the space they occupy should be considered an independent, freestanding forum for communicating protected speech, exclusive of the URL as a whole or other space within the URL.

Consequently, even if it were appropriate to view an Internet Web address as a "forum" at all, it would seem only logical to look at the entire URL--that is, the entire address--rather than one or more of its component parts (e.g., protocol identifier, top-level domain, second-level domain, directories, files, etc.). And, even assuming that a complete Internet URL could properly be construed to be a "forum" for speech, Network Solutions' decision to reject plaintiffs' applications to register the Disapproved Names as second-level domain names had no meaningful impact on their asserted First Amendment right to include whatever language they wished in their Web addresses, however profane or offensive to the public at large.

If they were interested in communicating some sort of message in their Web addresses, plaintiffs could easily accomplish that goal without the need to secure any approval from Network Solutions. First, they might append the desired "message" to their domain name by creating a directory on their Web server(s) with that particular name. So, for example, if plaintiff Haberstroh is truly interested in conveying some sort of message in her Web address, she could register the second-level domain name "Haberstroh.com" and create a directory entitled "tits" on her Web server. Thus, the URL for that particular site on the Internet would be (and would appear on the user's computer as): <http://www.haberstroh.com/tits>. Alternatively, she could use "tits" as her *third*-level domain name, with a resulting URL something like: <http://www.tits.haberstroh.com>. Neither process requires any input or approval from Network Solutions.

Similarly, National might register the domain name "National.com" or "photos.com." Then, it could simply create a directory or file entitled "feelmytits." Thus, its URL might be something like: <http://www.photos.com/feelmytits>. Or, as noted above, National could use that phrase as its third-level domain name (e.g., <http://www.feelmytits.photos.com>).

Regardless of whether plaintiffs placed their claimed protected "speech" in a file or directory or used it as part of a third-level domain name, whenever users clicked on a link to that page or whenever a search engine returned that page as a "hit," the complete URL (including plaintiffs' "message" or claimed protected speech) would appear on the user's monitor (either in the address bar or in the text displayed on the "results page" returned by the search engine). And, to the extent that the word "tits" or the phrase "feel my tits" are communicative, protected speech, those "messages" are successfully conveyed to the Internet user in the only "forum" even arguably relevant to this inquiry: the complete URL as displayed on the user's computer. Thus, contrary to plaintiffs' assertions, Network Solutions' refusal to register the Disapproved Names as second-level domain names did not constitute a "prior restraint" on protected speech.

In an analogous situation, the Court of Appeals for the Second Circuit considered a party's claimed First Amendment right to compel Network Solutions to create new generic *top*-level domain names (in addition to, for example, ".com"), such as ".forpresident." Recognizing that the

petitioners could simply register "forpresident" as a second or third-level domain name, the court observed that Network Solutions' conduct did not adversely affect their arguably protected speech:

**176 Here petitioners are not prevented from expressing their message in any one of several different ways. Currently, Name.Space is free to use any of an infinite possible number of second-, third and fourth-level domains as long as it has not previously been registered. The difference between ".forpresident" and ".forpresident.com," or ".net" or ".org" does not rise to the level of a prior restraint that offends the First Amendment.*

Name.Space, 202 F.3d at 587 (emphasis supplied). Similarly, even assuming that the Disapproved Names constitute protected speech, it is difficult to imagine how (or why) the difference between "tits.com" and "photos.com/tits" or the difference between "feelmytits.com" and "feelmytits.photos.com" either is or should be of constitutional significance.

At this point it is appropriate to discuss the apparent motivation underlying plaintiffs' efforts to secure the Disapproved Names as second-level domain names, as that is a defined factor in the applicable legal analysis. The record suggests that plaintiffs seek to register those particular second-level domain names so that Internet users might quickly and conveniently locate their particular websites, without the need to employ an Internet search engine. In other words, without knowing the URL of any particular website, a user interested in finding a site dedicated to providing sexually oriented material might make an educated guess and type in the URL: <http://www.tits.com>, with the reasonable expectation that he or she will discover a website dedicated to that anatomical subject. Similarly, a person interested in finding the website operated by International Business Machines might make an educated guess and type the address <http://www.IBM.com> hoping that he or she is taken to a site associated with IBM. Thus, by guessing at the likely content of various URLs one might often locate a website dedicated to a particular topic, without having to first conduct a search through a traditional search engine.

Consequently, plaintiffs' efforts to secure the Disapproved Names would seem to be motivated more by an interest in obtaining a topically relevant and easy- to-guess (and remember) "address" on the Internet than by a desire to communicate ideas or speech. And, while plaintiffs might easily create URLs that achieve the purported goal of communicating a protected message in their Web addresses, by doing so in space other than the top and second-levels they would lose the opportunity to secure the specific Web addresses they seek, which are more likely to be visited by people who are "guessing" at Web addresses in an effort to find those topically related to information they seek. For example, a user conducting a random search for sexually oriented websites, and who would rather guess at possible addresses than use a search engine, is far more likely to simply type <www.tits.com> rather than, say, < www.tits.photos.com>. Standing alone, however, the mere possibility that plaintiffs might, as a result of Network Solutions' conduct, realize less Internet traffic to their sites by people typing in assumed domain names, does not convert an otherwise invalid claim into one of constitutional significance. As the Court of Appeals for the Eleventh Circuit aptly observed, "the First Amendment does not guarantee anyone a profit. All it requires is that 'speech,' 'expression,' and 'ideas' be allowed a physically adequate forum." *Int'l Food & Beverage Systems v. City of Fort Lauderdale*, 794 F.2d 1520, 1526 (11th Cir.1986).

In light of the foregoing, even assuming that Network Solutions was a state actor, its declination to register the Disapproved Names has not adversely affected plaintiffs' rights to free speech in a constitutionally significant way. Plaintiffs may include in their Web addresses (i.e., the URLs)

whatever words or phrases they choose; no "speech" has been suppressed. *177 That plaintiffs insist upon using the second level domain space for "speech" by including the six words Network Solutions deems inappropriate (rather than simply appending phrases employing those words to their full URLs) makes it reasonably clear that they are not concerned with expressing a viewpoint or engaging in communicative speech within their Web addresses, but rather are seeking specific domain names that they believe will generate commercial Web traffic. Thus, what they have been denied is a convenient, easy-to-guess (and remember) "source identifier" or *pointer* to topical website(s). However, as other federal courts have concluded, that address/pointer is not entitled to constitutional protection:

Here, defendants' use of plaintiff's mark as the domain name for their web site is, on its face, more analogous to source identification than to a communicative message; in essence, the name identifies the web site as being the product, or forum, of the plaintiffs.

OBH, Inc. v. Spotlight Magazine, Inc., 86 F.Supp.2d at 198. *See also Planned Parenthood Federation of America, Inc. v. Bucci, supra* (S.D.N.Y.1997) (holding that the defendant's use of the second-level domain name "plannedparenthood.com" served only as a means by which to direct Internet users to his anti-abortion website, rather than any sort of communicative message, and therefore was not protected by the First Amendment). The district court's opinion in *Bally Total Fitness, supra*, is not to the contrary. That court concluded that, under particular circumstances, a URL (as distinguished from the discrete space occupied by a second-level domain name) may contain constitutionally protected speech--there, the URL in question was: <www.compix.com/ballysucks>. *Bally Total Fitness*, 29 F.Supp.2d at 1167-68.

As in *Planned Parenthood* and *OBH, Inc.*, here plaintiffs' proposed use of the domain name "tits.com" (and the other Disapproved Names) would serve merely to identify the source or address of plaintiffs' "product," site, or forum-- presumably a website dedicated to that particular topic whose purpose would be to communicate relevant information and materials. *See also PGMedia, Inc.*, 51 F.Supp.2d at 408 (concluding that a domain name is "simply a routing instruction that helps computers find each other."). And, of course, to the extent plaintiffs believe the Disapproved Names *are* actually communicative of some particular message, they remain free to include them in their URLs.

Accordingly, this case is not like those in which a party has been completely prohibited from communicating an arguably protected message in a recognized forum, such as, for example, the case in which the State of Missouri revoked a driver's "ARYAN-1" license plate. *See Lewis v. Wilson*, 89 F.Supp.2d 1082 (E.D.Mo.2000). *See generally Cohen v. California, supra*. Instead, this case is more analogous to those in which government action has had, at most, an insignificant impact on a person's freedom of speech. A good example of such cases are those in which a party has been refused trademark protection for an "immoral" or "scandalous" mark. *See generally* 15 U.S.C. § 1502 (providing that registration of a trademark may be refused if it "[c]onsists of or comprises immoral, deceptive, or scandalous matter."). For example, in *In re McGinley*, 660 F.2d 481 (Cust. & Pat.App.1981), the court concluded that the plaintiff's First Amendment rights were not violated when the Patent and Trademark Office refused to register a mark depicting exposed male genitalia.

With respect to appellant's First Amendment rights, it is clear that the PTO's refusal to register appellant's mark *does not affect his right to use it. No conduct is proscribed, and no tangible form of expression is suppressed.* Consequently, appellant's First Amendment rights would not be abridged by the refusal to register his mark.

*178 *Id.*, at 484 (emphasis supplied). See also *Ritchie v. Simpson*, 170 F.3d 1092, 1099 (Fed.Cir.1999) ("The dissent also expresses at some length concerns about Mr. Simpson's First Amendment rights. The dissent fails to understand that the denial of federal registration of a mark does not prohibit the use of that mark. Although the mark holder who is denied federal registration will not receive the benefits conferred on a federal trademark registrant, the mark holder may and can continue to use the mark."); *In re Mavety Media Group Ltd.*, 33 F.3d 1367 (Fed.Cir.1994) (rejecting a First Amendment challenge to the PTO's refusal to register the mark "BLACK TAIL"); *Lee v. Ventura County Superior Court*, 9 Cal.App.4th 510, 11 Cal.Rptr.2d 763 (1992) (holding that appellant had no constitutionally protected right to legally change his name to "Mister Nigger" and, because he retained the common law right to use that name, the State's refusal to officially sanction his name change did not adversely affect his First Amendment right to freedom of speech).

So it is in this case. No tangible form of expression has been suppressed by Network Solutions' refusal to register the Disapproved Names as second-level domain names. To the extent plaintiffs wish to use the Disapproved Names, they are at liberty to employ them in their URLs (e.g., as files or directories or as third-level domain names). Then, should a user click on a link to a page maintained by plaintiffs, the address displayed on the user's Internet browser's address bar would display that URL and would include whatever "message" plaintiffs choose to disseminate in that limited manner. Or, if one of the Web pages maintained by plaintiffs should be returned as a "hit" by a search engine, the URL for that page (again, including plaintiffs' asserted message) would be displayed on the user's monitor.

In short, plaintiffs' asserted free speech rights have not been infringed in any constitutionally significant way by the conduct of either Network Solutions or NSF. As suggested by the Court of Appeals for the Second Circuit, there is no constitutionally significant difference between, for example, <http:// www.tits.com> (an address prohibited by Network Solutions' conduct) and < http://www.tits.photos.com> (an address plaintiffs could have established, without intervention by or approval of Network Solutions). See *Name.Space*, 202 F.3d at 587.

Conclusion

Under the test adopted by the court of appeals in *Perkins*, Network Solutions was not a "state actor" when it rejected plaintiffs' applications to register the Disapproved Names as second-level domain names. Nevertheless, even assuming that Network Solutions was a state actor, plaintiffs' First Amendment rights were not violated.

To be sure, one might seek to use the space occupied by second-level domain names as a communicative vehicle, even though it was neither designed for that purpose nor intended to serve that function (e.g., "JonesForPresident.com"). However, in determining whether a Web address communicates speech protected by the First Amendment, there is no constitutional or even logical reason to parse the complete address into its component technical parts, and decide whether any one or more of those technical components--such as the space occupied by second-level domain names-- constitutes a discrete and free standing "forum" for speech, particularly when the complete address can accommodate (within its technical limitations) whatever "message" the designer might wish to fashion.

To the extent plaintiffs are actually intent upon expressing opinions, communicating messages, or encouraging public debate (rather than merely capturing Internet traffic) by including particular words or phrases in a Web address, Network Solutions' so-called decency policy does nothing to inhibit such speech. Plaintiffs remain free to include the Disapproved Names in the URLs associated *179 with whatever websites they might choose to operate. And, of course, to the extent plaintiffs are concerned with generating Web traffic at their sites, they remain free to use the Disapproved Names in traditional advertising as well as meta-tags embedded in the various pages located at those sites, thereby increasing the likelihood that search engines will direct users to plaintiffs' sites.

Perhaps more importantly, the *content* of any websites operated by plaintiffs is in no way affected by Network Solutions' refusal to register the Disapproved Names as second-level domain names. *See Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F.Supp. 949, 960 n. 4 (C.D.Cal.1997) ("It is important to note that impeding access to a domain name is not the same thing as impeding access to the Internet.... A Web site's content is not connected to or restricted by the domain name under which it is accessed."), *aff'd*, 194 F.3d 980 (9th Cir.1999). The real forum--and an essentially unregulated forum--is the website itself, over which Network Solutions exercised no editorial control.

In the end, therefore, plaintiffs' claim that they have a constitutionally protected right to include particular words or phrases in the space occupied by second-level domain names falls short. Plainly, URLs, transfer protocol identifiers, TLDs, and second-level domain names were not designed, intended, or traditionally employed to act as fora for speech. Second-level domain names like, for example, Social Security numbers or telephone numbers, serve an essentially utilitarian role: they enable a computer user to access a particular entity connected to the Internet, without the need to remember that entity's numerical IP address. That some people might want to express points of view or attempt to convey a particular message by converting the second-level domain name space into a message-carrying vehicle, does not operate to convert that space or the Domain Name System into a "forum" for speech. And, as discussed above, several important factors counsel against concluding that the space occupied by second-level domain names is, in and of itself, a discrete and cognizable forum for speech. Instead, to the extent that it is at all reasonable to view a Web address as a forum for speech, it is appropriate to look at the complete URL. In that "forum"--the complete URL--plaintiffs' speech has not been suppressed or inhibited in any constitutionally significant way by the complained-of conduct of Network Solutions or the NSF.

For the foregoing reasons, Network Solutions' motion for summary judgment (document no. 19) and the NSF's motion for summary judgment (document no. 51) are granted. Network Solutions' motion to dismiss National's amended complaint (document no. 56) is denied as moot. Haberstroh's motion for summary judgment (document no. 216) is denied. The Clerk of Court shall enter judgment in accordance with this order and close the case.

SO ORDERED.

END OF DOCUMENT