

# Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet

Markus Müller<sup>1</sup>

INTRODUCTION .....	710
I. U.S. POWER OVER THE INTERNET.....	713
A. <i>The Root File—The Decisive Point of Power</i> .....	713
B. <i>IP Addresses</i> .....	720
C. <i>TCP/IP</i> .....	722
D. <i>Backbone and Local Loop</i> .....	723
E. <i>Other Countries' Power in Comparison to the United States'</i> .....	724
F. <i>Summary of U.S. Power</i> .....	726
II. LIMITATIONS OF SOVEREIGNTY .....	727
III. DOES OWNERSHIP LEGITIMIZE U.S. POWER? .....	728
A. <i>Property Claim</i> .....	728
B. <i>Ownership of Tangible Things</i> .....	729
C. <i>U.S. Intellectual Property Law</i> .....	731
1. <i>TCP/IP and Copyright</i> .....	731
2. <i>TCP/IP and Patent Law</i> .....	734
3. <i>Root File and Copyright</i> .....	736
4. <i>Root File, DNS and Patent Law</i> .....	738
5. <i>Other Protection of the Root File</i> .....	738
6. <i>Summary of U.S. Intellectual Property Law</i> .....	742

---

<sup>1</sup> Postdoctoral Researcher, Law School, University of Tübingen, Germany. Dr. iur. (doctoral degree in law), University of Tübingen, 1999. LL.M., School of Law (Boalt Hall), University of California, Berkeley, 2002. Graduation from Law School (Rechtsreferendar), Munich University, 1996. I would like to thank Mark Lemley and Jane Winn for comments on an earlier draft.

D. <i>International Intellectual Property Law</i> .....	742
1. Software Patents in Treaties .....	743
2. Copyright Treaties .....	745
3. Trademark and Tort Law .....	746
CONCLUSION .....	747

## INTRODUCTION

The challenges that countries face when confronted with the Internet demonstrate the significance of Internet governance.<sup>2</sup> For example, “stricter” countries do not want their citizens to read Nazi books or are afraid of pornography, online gambling, or even of free speech in general. They see their sovereignty endangered by Web sites from other countries where such behavior is legal. On the other hand, “liberal” countries like the United States see their constitutional freedom of speech limited by the French court order in *L’Association Union des Etudiants Juifs de France v. Yahoo! Inc.*,<sup>3</sup> which declared it illegal for an American company to present

<sup>2</sup> The Internet is defined as the global computer network that uses TCP/IP protocols. DOUGLAS E. COMER, *COMPUTER NETWORKS AND INTERNETS* 615 (3d ed. 2001). To be on the Internet, a computer has to run the TCP/IP protocols, have a (temporary) IP address, and be able to send IP packets to other computers on the Internet. ANDREW S. TANENBAUM, *COMPUTER NETWORKS* 56 (4th ed. 2003). However, there is no fixed nature of the Internet. See LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 24–29, 30 (1999).

<sup>3</sup> See *L’Association Union des Etudiants Juifs de France v. Yahoo! Inc.*, T.G.I. Paris, Ordonnance de référé du 22 mai 2000, RG 00/05308, Legipresse Septembre 2000, No. 174 III, p. 142, available at <http://www.foruminternet.org/telechargement/documents/tgi-par20000522.pdf>; <http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm> (providing an English translation); *L’Association Union des Etudiants Juifs de France v. Yahoo! Inc.*, T.G.I. Paris, Ordonnance de référé du 11 août 2000, available at [http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord\\_tgi-paris\\_110-800.htm](http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi-paris_110-800.htm); cf. *Revue Lamy Droit des affaires* 2000, No. 31, No. 1979; *L’Association Union des Etudiants Juifs de France v. Yahoo! Inc.*, T.G.I. Paris, Ordonnance de référé du 20 novembre 2000, RG 00/05308, available at <http://www.foruminternet.org/telechargement/documents/tgi-par20001120.pdf> (Nov. 20, 2000); *League Against Racism and Antisemitism v. Yahoo! Inc.*, County Court of Paris (2000), available at <http://www.cdt.org/speech/international/001120yahoofrance.pdf> (Nov. 20, 2000) (providing an English translation); cf. *Revue Lamy Droit des affaires* 2001, No. 34, No. 2158.

Nazi books for sale on its American Web site because doing so is prohibited in France.

These are just a few examples of the policy issues in Internet governance, which can be summarized as decisions about what people are capable of doing, and allowed to do, on the Internet.<sup>4</sup> Policy issues concern domain names like `www.un.int`; technical standards such as architectural principles,<sup>5</sup> data formats,<sup>6</sup> and rules of transportation;<sup>7</sup> the use of encryption technology; and most importantly, content regulation with its free speech and privacy implications. Such policy questions are also reflected in the ongoing efforts to introduce the country-code top-level domain (TLD) “.ps” for Palestine,<sup>8</sup> and the decision about whether control of country-code TLDs such as “.af” for Afghanistan should be taken from the old national powers and handed over to the new powers during a war.<sup>9</sup> One last example of the implications of Internet governance is the limitation of characters in domain names to the English alphabet,<sup>10</sup> which excludes, for example, Chinese characters.

---

<sup>4</sup> The technical nature of the Internet results in the ability to make forbidden behavior literally impossible, i.e. having the capacity to do something and having the permission to do something may be indistinguishable. See LESSIG, *supra* note 2, at 89; WILLIAM J. MITCHELL, *CITY OF BITS* 111 (1995).

<sup>5</sup> Cf. Mark A. Lemley & Lawrence Lessig, *The End of End-To-End*, 48 *UCLA L. REV.* 925 (2001).

<sup>6</sup> XML is an example of a data format. See W3C, *Extensible Markup Language (XML)*, at <http://www.w3.org/XML> (last visited Nov. 15, 2004).

<sup>7</sup> In general, all data packets have the same priority but some wish for a discrimination between applications to guarantee a certain quality of service, which will often be a particular transfer speed. See RFC 2990. For details on RFCs see *infra* text accompanying note 58.

<sup>8</sup> Internet Assigned Numbers Auth., *Report on Request for Delegation of the .ps Top-Level Domain*, at <http://www.iana.org/reports/ps-report-22mar00.htm> (Mar. 22, 2000).

<sup>9</sup> Internet Assigned Numbers Auth., *Report on Redelegation of the .af Top-Level Domain*, at <http://www.iana.org/reports/af-report-08jan03.htm> (Jan. 8, 2003) (regarding the “Request of Islamic Transitional Government of Afghanistan for Redelegation of the .af Top-Level Domain”).

<sup>10</sup> *American Standard Code for Information Interchange*, at <http://www.argospress.com/Resources/CommunicationsSystems/abbrevA-ameristandacodforinformint-erc.htm> (last visited on Nov. 15, 2004) (defining ASCII as “code that uses seven bits to represent standard text characters as well as a number of terminal control characters such as line feed, carriage return and so on. American Standard Code for Information Interchange (pronounced “askey”) is one of the two common computer codes.”).

This Article concerns the basic control issue of Internet governance: Who should decide these policy questions? The *Yahoo!* case and the ongoing discussion about ICANN (Internet Corporation for Assigned Names and Numbers) exemplify the unresolved issue of control over the universal Internet. The United States has unique power over the Internet, which will be discussed in Part I. A need for a justification of U.S. power arises because many countries reject American control and demand that control over the Internet be handed over to the United Nations or, more specifically the International Telecommunications Union.<sup>11</sup> Part II explains that sovereignty, the most general legal basis of a country's power, does not sufficiently justify American control over the Internet. Part III then examines whether a property right would instead provide an adequate justification.

Does the United States own the Internet? There is a vague notion that the United States has the right to control the Internet because it is an American "thing" invented and funded by Americans.<sup>12</sup> This Article explores the merits of such a notion by analyzing its potential legal meanings and examining the law as it stood at the time the technologies were developed, while also considering the law as it stands today. The conclusion explains

---

<sup>11</sup> See Jennifer L. Schenker, *Nations Chafe at U.S. Influence over Internet*, N.Y. TIMES, Dec. 8, 2003, at C1; Jennifer L. Schenker, *U.N. Agrees to Examine How Internet is Governed*, N.Y. TIMES, Dec. 15, 2003, at C6; David McGuire, *U.N. Sets Aside Debate Over Control of Internet*, WASH. POST, Dec. 9, 2003, at E05; David McGuire, *U.N. Summit to Focus on Internet—Officials to Discuss Shifting of Control to International Body*, WASH. POST, Dec. 5, 2003, at E05; cf. also Gregory R. Hagen, *Sovereign Domains and Property Claims*, 11 INT'L J.L. & INFO. TECH. 1 (2003) (arguing that countries should seek full control of country code TLDs).

<sup>12</sup> Though this claim may not necessarily be the official policy of the U.S. government, some agree with it. See David R. Johnson & David Post, *Law and Borders*, 48 STAN. L. REV. 1367, 1393 (1996) ("A U.S. government representative has stated that, since the government paid for the initial development and administration of the domain name system, it 'owns' the right to control policy decisions regarding the creation and use of such names."); Yochai Benkler, *Internet Regulation*, 11 EUR. J. INT'L L. 171, 172, 175, 179 (2000); *The Governance of the Domain Name System by the Internet Corporation for Assigned Names and Numbers Before the Subcomm. on Telecomm. of the U.S. Sen. Commerce Comm.* 107th Cong. (Feb. 14, 2001) (testimony of Brian R. Cartmell, Chief Executive Officer, eNIC Corp.), at <http://www.senate.gov/~commerce/hearings-0214car.pdf>; see also Schenker, *Nations Chafe at U.S. Influence over Internet*, supra note 11 (discussing U.S. ownership of Internet resources).

what the Article's ownership analysis means for the possibility of justifying the United States' special power with the Internet being an American gift to the world and then demonstrates the limitations of national power with respect to global public goods.

## I. U.S. POWER OVER THE INTERNET

This Part demonstrates the United States' power in Internet governance by examining its level of control over each component of the Internet's infrastructure. The infrastructure of the Internet consists of the Domain Name System (DNS), with the root file at the top of its hierarchy, IP addresses, the TCP/IP protocols, the backbone, and the local loop. Control over each of these individual components results in a different level of power over the Internet as a whole. An analysis of the infrastructure reveals why the United States has so much power and prepares the groundwork for the ownership analysis, by showing what the Internet consists of and what aspects of it can be owned in the first place.

### A. *The Root File—The Decisive Point of Power*

The root file is the core element of the DNS and of the United States' power over the Internet. This section begins by describing the DNS and the root file and why having control over it translates into substantial power over the Internet. Following this, it explains the United States' control over the root file.

The Internet is a network of networks and consists of about 500,000 subnetworks.<sup>13</sup> A computer network requires an address system. The address system of the Internet has two dimensions: the IP address and the domain name. Every computer connected to the Internet has an IP address, even if only a temporary one.<sup>14</sup> An IP address is a thirty-two bit number usually written in dotted decimal notation like 233.64.133.130 and used like a mail address to deliver data packets between the computers.<sup>15</sup> IP addresses are

---

<sup>13</sup> TANENBAUM, *supra* note 2, at 437.

<sup>14</sup> See TANENBAUM, *supra* note 2, at 56.

<sup>15</sup> TANENBAUM, *supra* note 2, at 437; JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING 123 (3d ed. 2004).

hard for people to remember. Therefore the Domain Name System (DNS) was developed.<sup>16</sup> The DNS allows people to use mnemonic identifiers, which are called domain names (e.g., www.un.int), instead of an IP address.<sup>17</sup> In order to exchange data with another computer, the domain name of the second computer must be translated into its IP address because the Internet's transport system itself understands only IP addresses.<sup>18</sup> The widespread use of domain names as a proxy for IP addresses makes them a valuable resource. A computer connected to the Internet can always be reached via its IP address, but its visibility to Internet users is reduced if it cannot be reached via a domain name as well because people are less likely to memorize IP addresses.

The DNS assigns domain names to IP addresses and informs querying computers which IP address belongs to a particular domain name—a process called name resolving.<sup>19</sup> Domain names are unique<sup>20</sup> and have a hierarchical structure like a tree.<sup>21</sup> The last part of each domain name, e.g. “.com”, indicates the Top-Level-Domain (TLD) the domain name belongs to. There are fourteen generic TLDs like “.com” and around 244 country-code TLDs like “.uk.”<sup>22</sup> The second-to-last part of a domain name, e.g. berkeley in www.berkeley.edu, is called second level domain and indicates the subdomain berkeley in the TLD .edu.

The two decisive components of the DNS are the root file and name servers.<sup>23</sup> The root file, also called “the dot,” contains the authoritative information about TLDs. The root file lists all TLDs

---

<sup>16</sup> For additional reasons, see TANENBAUM, *supra* note 2, at 579.

<sup>17</sup> See MILTON L. MUELLER, RULING THE ROOT 39 (2002).

<sup>18</sup> See TANENBAUM, *supra* note 2, at 579; MUELLER, *supra* note 17, at 5–6.

<sup>19</sup> See Request for Comments [hereinafter RFC] 1034, pp. 5, 21.

<sup>20</sup> See RFC 2826, p. 1 (deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations); A. Michael Froomkin, *Wrong Turn in Cyberspace*, 50 DUKE L.J. 17, 44 (2000); TANENBAUM, *supra* note 2, at 436. IP addresses are also unique.

<sup>21</sup> See RFC 1034, pp. 5, 9.

<sup>22</sup> See MUELLER, *supra* note 17, at 41–43, 204; Froomkin, *supra* note 20, at 37–40; Internet Assigned Numbers Auth., *Generic Top-Level Domains*, at <http://www.iana.org/gtld/gtld.htm> (last updated Oct. 28, 2004).

<sup>23</sup> Another important part is the root hints data, see Paul Albitz & Cricket Liu, DNS and BIND 67 (4<sup>th</sup> ed. 2001).

and, for each TLD, the name server, which stores a list of the (second-level) domain names of the TLD along with their corresponding IP addresses.<sup>24</sup> By referring to a particular name server, the root file gives that name server control over the domain names in that TLD. The following excerpt from the root file serves as an illustration:

```
“. IN SOA A.ROOT-SERVERS.NET.  
NSTLD.VERISIGN-GRS.COM.
```

```
[. . .]
```

```
MUSEUM. NS NIC.ICOM.ORG.
```

```
[. . .]
```

```
NIC.ICOM.ORG. A 195.7.65.253”25
```

The root file determines that all (second-level) domain names ending with .museum are stored with their IP addresses<sup>26</sup> on the name server NIC.ICOM.ORG, which has the IP address 195.7.65.253. All domain names depend on the root file because it refers searching computers to particular name servers and, thus, gives these name servers the authority to assign domain names under the TLDs. The original root file is stored on the “A-root-server” of the company NSI-Verisign in Virginia.<sup>27</sup> As a practical matter this root file is authoritative because other computers accept and follow it.<sup>28</sup>

---

<sup>24</sup> See Froomkin, *supra* note 20, at 43; MUELLER, *supra* note 17, at 47.

<sup>25</sup> The first way to retrieve the root file is the Unix command “dig @f.root-servers.net . axfr”. See RFC 1035, p. 13 (explaining command axfr); Albitz & Liu, *supra* note 23, at 401. This command is blocked at the a.root-server. See RFC 2870. The second way is to download it from ftp.rs.internic.net/domain/root.zone.gz or ftp://ftp.internic.net/domain. Cf. *Using the Downloads*, [http://www.cisco.com/public/sw-center/sw\\_download\\_guide/dnsfaq.shtml](http://www.cisco.com/public/sw-center/sw_download_guide/dnsfaq.shtml) (last visited Apr. 5, 2005); ELLEN RONY & PETER RONY, *THE DOMAIN NAME HANDBOOK*, 81–85 (1998).

<sup>26</sup> See RFCs 1034, 1035. Often the name server will just point to another computer lower in the hierarchy. See KUROSE & ROSS, *supra* note 15, at 127.

<sup>27</sup> See MUELLER, *supra* note 17, at 41–43, 204; Froomkin, *supra* note 20, at 37–40; Internet Assigned Numbers Auth., *Generic Top-Level Domains*, at <http://www.iana.org/gtld/gtld.htm> (last updated Oct. 28, 2004). Twelve other servers mirror this data. See David Conrad et al., *Root Nameserver Year 2000 Status*, at <http://www.icann.org/committees/dns-root/y2k-statement.htm> (July 15, 1999).

<sup>28</sup> See Froomkin, *supra* note 20, at 43.

The reason other people follow the root file on the A-root-server is the key to understanding the power structure of the DNS. A unified worldwide Internet provides network gains that would not be achieved by several separate networks.<sup>29</sup> Not following the root file means to risk a split of the root;<sup>30</sup> the Internet would no longer be a universal network because Internet users, although using the same domain name, would no longer always be connected to the same computer or Web site. Someone who considers introducing an alternative root faces a difficult decision because if too few players follow, he will end up with an isolated network without great network gains for its participants.<sup>31</sup> Therefore, the root file stored at NSI-Verisign has a tremendous first-mover advantage.<sup>32</sup>

The power derived from control of the root file is most obvious with respect to the introduction of new TLDs. A new TLD like “.ps” for Palestine is only functional if it is included in the root file, because only then will the DNS direct users to IP addresses that belong to second-level domain names ending with .ps.<sup>33</sup>

---

<sup>29</sup> A network effect or positive externality is present if the utility for each user of the good increases with the number of other people using the good. Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985). For example, the value of participating in a communications system to one user is positively affected when other users join and enlarge the network. Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 93–94 (1994).

<sup>30</sup> See Froomkin, *supra* note 20, at 45–46.

<sup>31</sup> For arguments against alternative roots, see RFC 2826; M. Stuart Lynn, *A Unique, Authoritative Root for the DNS*, at <http://www.icann.org/icp/icp-3.htm> (July 9, 2001).

<sup>32</sup> See CARL SHAPIRO & HAL R. VARIAN, *INFORMATION RULES*, 29–32, 168–69 (1999) (information on first-mover advantages). First-mover advantages have made alternative roots unsuccessful. See MUELLER, *supra* note 17, at 50–56.

<sup>33</sup> The European Union faced difficulties representing itself with “.eu” because ICANN, which obtained some control over the root file from by the U.S. government, at first deemed it inappropriate based on the list of countries by the International Organization for Standardization, which does not contain the European Union. Now EU appears on ISO’s reserved list. Int’l Org. for Standardization, *English Country Names and Code Elements*, at <http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html> (last visited Apr. 4, 2005); Letter from Michael M. Roberts, President, ICANN, to Erkki Liikanen, Commissioner, European Commission, Regarding .eu Top-Level Domain (Aug. 10, 2000), at <http://www.icann.org/correspondence/roberts-letter-to-liikanen-10aug00.htm>; ICANN, *.EU Update*, at <http://www.icann.org/announcements/announcement-23mar05.htm> (Mar. 23, 2005).

Conversely, if a TLD was removed from the root file and the other name servers in the DNS followed the change, this TLD would no longer be accessible using domain names.

The United States controls the root file because the A-root-server is located in the United States, thus precluding other governments from physical access,<sup>34</sup> and also because NSI-Verisign, which physically controls the A-root-server, is contractually obligated to secure written approval from the U.S. Department of Commerce before adding any TLDs to the root.<sup>35</sup> This gives the United States the capacity to threaten a country with the prospect of taking away its country-code TLD.<sup>36</sup>

The DNS and in particular the introduction of new TLDs are managed by ICANN, a nonprofit corporation that is incorporated and based in California.<sup>37</sup> Although people from all over the world have functions in ICANN, ICANN's role in the realm of Internet governance has not reduced the power of the U.S. government because the original plan ("Green Paper")<sup>38</sup> to transfer full control to a new, independent entity was never implemented<sup>39</sup> and ICANN

---

<sup>34</sup> Several of the other root-servers, which mirror the A-root-server, are located in the United States as well.

<sup>35</sup> *Cooperative Agreement between NSI and U.S. Government*, Amend. 11, at <http://www.icann.org/nsi/coopagmt-amend11-07oct98.htm> (Oct. 7, 1998) [hereinafter *NSI-U.S. Cooperative Agreement*, Amend. 11] ("NSI . . . shall request written direction from an authorized [U.S. government] official before making or rejecting any modifications, additions or deletions to the root zone file.").

<sup>36</sup> The U.S. government has no explicit contractual right to order NSI to delete a TLD. But its right to veto any change gives it such a strong bargaining position that NSI-Verisign could not resist. Additionally, NSI-Verisign depends on the government in antitrust matters. See *infra* text accompanying note 72.

<sup>37</sup> *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers, as Revised*, § 3, at <http://www.icann.org/general/articles.htm> (Nov. 21, 1998).

<sup>38</sup> See U.S. Dep't of Commerce, Nat'l Telecomm. & Info. Admin. ("NTIA"), Improvement of Technical Management of Internet Names and Addresses, Proposed Rule ("Green Paper"), 63 Fed. Reg. 8825 (Feb. 20, 1998). The Green Paper was followed by the "White Paper." U.S. Dep't of Commerce, Nat'l Telecomm. & Info. Admin. ("NTIA"), Management of Internet Names and Addresses, Statement of Policy, 63 Fed. Reg. 31741 (June 10, 1998).

<sup>39</sup> See U.S. Dep't of Commerce, Nat'l Telecomm. & Info. Admin. ("NTIA"), *Fact Sheet*, at <http://www.ntia.doc.gov/ntiahome/domainname/agreements/summary-factsheet.htm> (last visited Apr. 4, 2004) ("Nothing in these agreements affects the current arrangements regarding management of the authoritative root server. . . . The Department of Commerce has no plans to transfer to any entity its policy authority to direct the

still needs de facto approval of the U.S. government for any major decisions.<sup>40</sup> Any control ICANN has over the root file is still based on the will of the U.S. government, especially because it is the U.S. government that instructs NSI-Verisign to follow ICANN's policy.<sup>41</sup> The most significant reason why ICANN lacks independent power is that the U.S. government transferred the management of the DNS to ICANN by a time-limited contract that can be terminated by the U.S. government within 120 days.<sup>42</sup> In the event of termination, ICANN is obligated to assign to the U.S.

---

authoritative root server.”); *Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers*, (“DOC-ICANN Understanding”), Amend. 6, § I.B.14., at [http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6\\_09162003.htm](http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6_09162003.htm) (Sept. 16, 2003) (demonstrating that the U.S. government supports privatizing the technical management); Letter from Robert P. Murphy, General Counsel, U.S. Gen. Accounting Office, to Judd Gregg, Chairman, Subcomm. on Commerce, Justice, State, & the Judiciary, Comm. on Appropriations, U.S. Senate, et al. 25–30 (July 7, 2000) (on the relationship of the between the Department of Commerce and ICANN), at <http://www.gao.gov/archive/2000/og00033r.pdf>; MUELLER, *supra* note 17, at 197.

<sup>40</sup> See *Contract between ICANN and the United States Government for Performance of the IANA Function*, at <http://www.icann.org/general/iana-contract-21mar01.htm> (Mar. 21, 2001). In this contract, provisions 2.1.1.2 and 4.1 refer to the *Cooperative Agreement between NSI and U.S. Government*, Amend. 11, and thereby make clear that ICANN accepts the last word of the U.S. government. See *NSI-U.S. Cooperative Agreement*, Amend. 11, *supra* note 35. Furthermore, ICANN needs prior approval from the U.S. government for some registry agreements. See *Memorandum of Understanding between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers* (“DOC-ICANN Understanding”), Amend. 1, §§ 1, 2, 4, at <http://www.icann.org/general/amend1-jpamou-04nov99.htm> (Nov. 10, 1999); *DOC-ICANN Understanding*, Amend. 3, §§ I, II, at <http://www.icann.org/general/amend3-jpamou-25may01.htm> (May 25, 2001). To merely use the mark InterNIC, ICANN had to sign a license agreement with the U.S. government. See *License Agreement Concerning InterNIC*, at <http://www.icann.org/general/internic-license-08jan01.htm> (Jan. 8, 2001).

<sup>41</sup> See *NSI-U.S. Cooperative Agreement*, Amend. 11, *supra* note 35 (at section entitled “Recognition of NewCo”); *Cooperative Agreement between NSI and U.S. Government*, Amend. 19, § B. 1. (“ICANN as NewCo”), at <http://www.icann.org/nsi/coopagmt-amend19-04nov99.htm> (Nov. 10, 1999); *Special Award Conditions*, Amend. 24, at [http://www.ntia.doc.gov/ntiahome/domainname/agreements/amend24\\_52501.htm](http://www.ntia.doc.gov/ntiahome/domainname/agreements/amend24_52501.htm) (last visited on Nov. 15, 2004) (Verisign stepped into NSI's role which became a subsidiary).

<sup>42</sup> See *DOC-ICANN Understanding*, § VII, at <http://www.icann.org/general/icann-mou-25nov98.htm> (Nov. 25, 1998); *DOC-ICANN Understanding*, Amend. 2, § II, at <http://www.icann.org/general/amend2-jpamou-07sep00.htm> (Aug. 30, 2000); *DOC-ICANN Understanding*, Amend. 4, § I, at <http://www.icann.org/general/amend4-jpamou-24sep01.htm> (Sept. 24, 2001).

government any rights that ICANN has in all existing contracts with registries and registrars.<sup>43</sup>

To obtain the overall picture of U.S. power it is necessary to look at how the United States, through ICANN, has a grip on the entire world by a chain of contracts. ICANN imposes contractual obligations on all domain name holders in the space of TLDs like .com, .net, .org, and the newly introduced generic TLDs like .museum. Users can register domain names only with “registrars,” which in turn have to register them with the “registry” that is the highest level administrator of a TLD chosen by ICANN.<sup>44</sup> First, through contracts, ICANN can force all registries of generic TLDs to deal only with ICANN-accredited registrars, i.e. with entities subject to contractual obligations imposed by ICANN.<sup>45</sup> Second, ICANN’s contracts with the registrars require them to include certain obligations on the registrants (the individual domain name holders).<sup>46</sup> Currently the most important example of the power that the United States and ICANN derive from controlling the root file is the enforcement of the Uniform Domain Name Dispute Resolution Policy (UDRP), which is a set of rules for conflicts between trademark and domain-name holders.<sup>47</sup>

---

<sup>43</sup> See *DOC-ICANN Understanding*, Amend. 1, *supra* note 40, § 5; *DOC-ICANN Understanding*, Amend. 3, § IV, at <http://www.icann.org/general/amend3-jpamou-25may01.htm> (May 25, 2001).

<sup>44</sup> See *FAQs*, at <http://www.icann.org/faq> (last visited on Apr. 4, 2005).

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

<sup>47</sup> See *Uniform Domain Name Dispute Resolution Policy*, at <http://www.icann.org/udrp/udrp-policy-24oct99.htm> (Oct. 24, 1999) [hereinafter *UDRP*]. Registries are only allowed to register domain names for ICANN-accredited registrars. See *.com Registry Agreement*, § II.23-4, at <http://www.icann.org/tlds/agreements/verisign/registry-agmt-com-25may01.htm> (May 25, 2001). The registrar-accreditation agreement obligates registrars to incorporate the UDRP into contracts with domain-name holders (registrants), who are in turn forced to accept the UDRP. *Registrar Accreditation Agreement*, §§ 3.7.7.11, 3.8, at <http://www.icann.org/registrars/ra-agreement-17may01.htm> (May 17, 2001); *Policies Applicable to ICANN-Accredited Registrars*, at <http://www.icann.org/general/consensus-policies.htm> (last visited Nov. 15, 2004). It is estimated that the UDRP is imposed on about 70% of all registered domain names. Milton Mueller, *Rough Justice: A Statistical Assessment of ICANN's Uniform Dispute Resolution Policy*, 17 INFO. SOC'Y 151, 153 (2001) [hereinafter *Mueller, Rough Justice*]. ICANN has less power in terms of country-code TLDs. The few contracts entered into with ICANN by country-code registries like Australia's do not include an obligation to impose the UDRP. *ccTLD Sponsorship Agreement (.au)*, at <http://www.icann.org/cctlds/au/sponsorship>

### B. IP Addresses

The United States derives less power from the allocation of IP addresses than it does from the root file. This section first looks at the technical background, and then at ICANN's and the United States' control of IP addresses.

If an entity had a monopoly in allocating IP addresses and the technical capability to take them away, this entity would be able to control all activity on the Internet because an IP address is indispensable for any use of the Internet. This is not the case, however, because the IP address system works differently than the DNS. Routers, which are the computers that direct the data traffic of the Internet between the sub-networks, use IP addresses and are not hierarchically organized like the name servers of the DNS. The routers belong to backbone providers and Internet Service Providers, which provide users with connections to the network. The Internet is a network of networks; every network that is part of the Internet is physically connected to at least one other network. Other networks act as intermediaries in order to deliver data between networks that are not directly connected to one another.<sup>48</sup> In this case, the originating networks need only to know which of the networks it is connected to is in the position to deliver the information packet closer to its destination. Accordingly, routers do not have a list of all IP addresses but are programmed by each network individually with information to efficiently deliver the data to the networks it is connected to.<sup>49</sup> There is no central

---

agmt-25oct01.htm (Oct. 25, 2001). Note that Recitals 4.5.1–.2 concern only technical issues if registration from non-residents is not encouraged. *Id.* Recital 5.1 refers to Attachment F, which only restricts the use of punctuation within domain names. *Id.*; *ccTLD Sponsorship Agreement (.au)*, Attachment F, at <http://www.icann.org/cctlds-au/sponsorship-agmt-attf-25oct01.htm> (Oct. 25, 2001). With respect to other country-code TLDs, ICANN only has power derived from control over the root file and no contractual powers. The UDRP favors trademark holders compared to national and international trademark law. Mueller, *Rough Justice*, *supra*; Milton Mueller, *Success by Default: A New Profile of Domain Name Trademark Disputes under ICANN's UDRP*, at <http://dcc.syr.edu/markle/markle-report-final.pdf> (June 24, 2002); Michael Geist, *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903 (2002).

<sup>48</sup> Cf. ILJITSCH VAN BEIJNUM, BGP 228 (2002).

<sup>49</sup> 1 DOUGLAS E. COMER, INTERNETWORKING WITH TCP/IP 57, 119 (4th ed. 2000).

routing table that is copied to all routers;<sup>50</sup> it is a decentralized structure without any central on/off switch. Therefore, there is no easy way to cut an IP address off from the Internet. In order to do so, the IP address must become “invalid,” which occurs when the routers of the computer’s network dismiss the data packets or the network itself gets disconnected. This is in the hands of the network and the networks it is connected to, but there is no central authority that can easily disconnect an IP address.

IP addresses are allocated on several levels, with ICANN on top. ICANN allocates large blocks of IP addresses to four Regional Internet Registries, which in turn give them to users.<sup>51</sup> For ICANN, having control over an IP address means others are barred from using it without permission. It is only by convention, however, that ISPs do not use an IP address without permission because there is no technical obstacle to prevent them from doing so. Nevertheless, ISPs do not use reserved or otherwise allocated IP addresses.<sup>52</sup> The rationale behind this is that it is better to prevent chaos and rely on cooperation. Otherwise, people would start using other people’s IP addresses. This need for order creates a structure. The evolution of this structure is a case of private ordering driven by network gains for all involved ISPs and their

---

<sup>50</sup> Sometimes an “Internet Routing table” is mentioned. See Geoff Huston, *Analyzing the Internet BGP Routing Table*, 4 (1) INTERNET PROTOCOL J. (Mar. 2001). This is not a routing table with complete IP addresses used on routers directing the traffic on the Internet, but the product of some calculation for analytical purposes. The same is true for the Internet Routing Registry, which combines databases of routing policies. Cf. Merit Network, Inc., *Internet Routing Registry*, at <http://www.irr.net>; Request for Comments (“RFC”) 2904, p. 16 (RFCs are available on the internet at <http://www.rfc-archive.org>). Route servers at network access points are in some sense central points. See I COMER, *supra* note 49, at 287. But this is not comparable to the root file. For more information on routing, see also RAVI MALHOTRA, *IP ROUTING* (2002); SAM HALABI, *INTERNET ROUTING ARCHITECTURES* (2d ed. 2001). I thank Paul Hoffman for providing me with information.

<sup>51</sup> See RFC 2901, p. 7; Daniel Karrenberg et al., *Development of the Regional Internet Registry System*, 4 (4) INTERNET PROTOCOL J. (Dec. 2001), at [http://www.cisco.com/warp/public/759/ipj\\_4-4/ipj\\_4-4\\_regional.html](http://www.cisco.com/warp/public/759/ipj_4-4/ipj_4-4_regional.html); Mirjam Kühne, Slide Show, *Regional Registries System*, at <http://www.ripe.net/info/ncc/presentations/afrinicripe/sld001.html> (last visited on Apr. 4, 2005).

<sup>52</sup> A separate issue is the internal use.

customers.<sup>53</sup> Arguably, there is no need for ICANN to become involved as a centralized authority in this process.

ICANN does not have physical control over the network connections or router tables, nor does it have a contract that guarantees control.<sup>54</sup> Nevertheless, ICANN (and thereby the United States), has some power because many ISPs are part of the contractual chain of the DNS and therefore dependent on the goodwill of ICANN. Furthermore, someone who deviates from ICANN's allocation risks conflicting use of IP addresses, resulting in chaos. Such a move away from ICANN could only be done collectively by all of the entities involved in the transport of data, because they would have to agree upon a new way to coordinate the allocation of IP addresses—a scenario that is unlikely to take place. Thus the United States, through ICANN, derives some power over the Internet from the allocation of IP addresses, though considerably less than from the root file.

### C. TCP/IP

In order to participate in the Internet, a computer must use the TCP/IP protocols, which are rules for communication between computers that have been set as Internet standards by the standard-setting organization IETF (Internet Engineering Task Force).<sup>55</sup>

---

<sup>53</sup> ISPs have a strong incentive to avoid a split of the Internet that would make it less attractive for users.

<sup>54</sup> Cf. *Address Supporting Organization Memorandum of Understanding*, at <http://www.aso.icann.org/docs/aso-mou.html> (Oct. 18, 1999) (not providing ICANN with the right to give the Regional Internet Registries orders). ICANN and the Regional Internet Registries have so far not entered a contract and therefore, the Regional Internet Registries are not obligated to follow ICANN's wishes. Am. Registry for Internet Numbers, *Notice Concerning Contract between ICANN and the Regional Internet Registries*, [http://www.arin.net/announcements/04022002\\_newsletter.html](http://www.arin.net/announcements/04022002_newsletter.html) (Apr. 2, 2002); Am. Registry for Internet Numbers, *ARIN and ICANN Relationship Agreement*, [http://www.arin.net/library/internet\\_info/contract\\_chronology.html](http://www.arin.net/library/internet_info/contract_chronology.html) (last visited Nov. 15, 2004); *ICANN's Major Agreements and Related Reports*, at <http://www.icann.org/general/agreements.htm> (last visited Nov. 15, 2004) (no contract mentioned). In particular, ICANN has no contractual basis to regain control of allocated IP addresses.

<sup>55</sup> On the IETF, see The Internet Engineering Task Force, at <http://www.ietf.org> (last visited on Apr. 5, 2005); RFC 2026; RFC 3160; S. Bradner, *The Internet Engineering Task Force*, in *OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION* 47–52 (C. DiBona et al. eds., 1999). Because the IETF lacks any enforcement power it offers rather than sets the standards.

TCP and IP were published in 1981 as RFC 791 and RFC 793.<sup>56</sup> RFCs<sup>57</sup> are a series of documents on computer networking.<sup>58</sup> Many technical Internet standards, in particular the ones set by the IETF, have been published as RFCs; the RFC series is today the basic publication series for the IETF.<sup>59</sup>

The IETF is not under control of the U.S. government. However, if the U.S. government forced all people living in the United States to use a different standard, people in other countries would be forced to follow in order to communicate with people in the United States. Therefore, the United States has some power over these standards because most countries can hardly afford not to communicate with the United States via the Internet.<sup>60</sup>

#### *D. Backbone and Local Loop*

The backbone (big conduits between ISPs) and the local loop (typically a telephone line between user and ISP) are the indispensable physical means to transport data. Control over them would enable one to cut off users and translate into complete control of the Internet. However, U.S. control over the backbone and the local loop is limited to the parts located in its territory, thus making the backbone and the local loop relatively insubstantial sources of U.S. power.<sup>61</sup>

---

<sup>56</sup> IP is specified in RFC 791, published 1981, and updated by RFC 1349. TCP is specified in RFC 793, published 1981, and updated by RFC 3168.

<sup>57</sup> Bradner, *supra* note 55 at 50 (“RFC once stood for ‘Request for Comments,’ but since documents published as RFCs have generally gone through an extensive review process before publication, RFC is now best understood to mean ‘RFC.’”).

<sup>58</sup> RFC 2555, p. 2. RFCs are available on the Internet at <http://www.ietf.org/rfc.html> and <http://www.rfc-editor.org/> (last visited November 15, 2004).

<sup>59</sup> Bradner, *supra* note 55 at 50; RFC 2026, p. 6. The RFC series is older than the IETF. For names of and details on the organizations involved in the IETF standard-setting process, see RFC 3160 and RFC 2028.

<sup>60</sup> This power is less based on the unshared control of a key resource, the root file, than on a strong bargaining position with respect to a network good.

<sup>61</sup> Foreign companies owning parts of the local loop or the backbone outside the United States are to some degree under U.S. control if they are also in the business of domain name registration.

*E. Other Countries' Power in Comparison to the United States'*

Other countries have substantial power, but such power is limited by several factors. Each country has power from its control over the backbone and the local loop in its respective territory, which allows it to block physical access to the Internet. This is less true for access via satellites and international telephone connections because controlling satellite connections is a technical challenge and filtering all international telephone connections requires substantial effort. However, even if a pure technical solution for control is not airtight, a government can still exert substantial control by making trafficking in, and possession of, the necessary equipment a crime. Gaining control depends then on the will and resources of law enforcement. ISPs can be subjected to any regulation possible in the country because their physical presence is required to offer service.<sup>62</sup> Web sites also can be subjected to a country's regulations, if the server is located in that country.

Even foreign Web sites are not always completely out of the reach of a country's power. Many countries apply some of their laws to foreign Web sites that can be accessed in the country.<sup>63</sup> When a Web site owner has assets in a foreign country or does not want to lose the opportunity to visit it, they will be responsive to its regulations.<sup>64</sup> Such a reach of power can be illustrated by the reaction of the American company Yahoo! to an order by a French court to take down illegal material from its Web site.<sup>65</sup> Even though Yahoo! filed a successful lawsuit in the United States to prevent the enforcement of the French decision in the United

---

<sup>62</sup> Foreign ISPs are not under direct control but the connections to them are.

<sup>63</sup> See *supra* note 3 and accompanying text (French cases involving Yahoo); see, e.g., BGHSt 46, 212 (This decision of the highest German court enforcing German criminal law (Bundesgerichtshof) concerns the denial of the Nazi extermination of the Jews ("Auschwitzlüge"). It stated that it is the effect in Germany that is crucial in determining whether the law was violated, but not the location of the server, which was in Australia.).

<sup>64</sup> Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216 (1998).

<sup>65</sup> See Doug Isenberg, *Struggling with the French Yahoo Nazi-Auction Decision*, at <http://www.gigalaw.com/articles/2001-all/isenberg-2001-01b-all.html> (last visited Apr. 5, 2005).

States,<sup>66</sup> Yahoo! nevertheless complied with the French court's order.<sup>67</sup>

There are two major limitations to a national government's power. First, while it has the power to pull the plug on Internet access, as North Korea did,<sup>68</sup> it cannot single-handedly influence the content of foreign Web sites. Attempts to filter the data flow from other countries come at a price: success is uncertain, the performance of the data flow suffers, and the filter may often dismiss valuable material.<sup>69</sup>

The second limitation is caused by the structure of the DNS. Even the country-code TLDs are dependent on the root file that is only under U.S. control.<sup>70</sup> A country could force all computers within its territory to follow a new DNS, but that would not apply to computers anywhere else. A country can therefore threaten the United States with a split of the Internet in two parts and thereby cause the loss of network gains,<sup>71</sup> but it cannot alter the DNS for the whole Internet. In contrast, the United States, by virtue of its control of the root file, can cause great difficulties for a country by transferring the authority for the country-code TLD to an entity outside that country. The new, foreign entity would be able to program its now controlling name servers to stop referring to the "old" corresponding IP addresses, and thereby cancel all current

---

<sup>66</sup> *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (decision in favor of Yahoo), *rev'd*, 379 F.3d 1120 (9th Cir. 2004) (reversing for lack of personal jurisdiction over defendants), *reh'g en banc granted* 399 F.3d 1010 (case will be reheard en banc).

<sup>67</sup> The lawsuit was symbolic. The case shows the necessity to distinguish for analytical purposes between ways to enforce national law depending on whether they require cooperation of other countries.

<sup>68</sup> See REPORTERS SANS FRONTIERS & TRANSFERT.NET, ENEMIES OF THE INTERNET 79 (2001).

<sup>69</sup> See *Internet Filtering in Saudi Arabia in 2004*, at <http://www.opennetinitiative.net/studies/saudi> (last visited Apr. 6, 2005) (describing Saudi Arabia's efforts to filter content from Web sites).

<sup>70</sup> This is true despite the fact that nobody interferes with national decisions about the domain name structure in their respective domains such as .co.uk. See *supra* note 47 (providing information on insignificant restrictions for domain names in the new country-code TLD contracts with ICANN).

<sup>71</sup> The smaller the country, the greater the loss it suffers. For an explanation of network gains, see generally *supra* note 29.

domain names.<sup>72</sup> In response, a country can only resort to creating its own DNS and accept the inevitability of a split of the Internet.

Finally, although countries participate in ICANN as advisors,<sup>73</sup> their influence is very limited. The same is true with respect to the United Nations or other supranational organizations like the International Telecommunications Union (ITU), because these organizations do not have any particular power over the Internet.<sup>74</sup> Thus the power of other countries is overall relatively limited compared to the United States’.

#### F. Summary of U.S. Power

The implications of U.S. control over the Internet’s infrastructure are far-reaching. For better or for worse, the United States has (at least) delayed the original time plan to transfer full control of the root file to ICANN.<sup>75</sup> Through its control over the root file, and over IP addresses (although to a much lesser extent), as well as any potential influence over the TCP/IP protocols, the United States has a power over the Internet unrivaled by any other nation.<sup>76</sup> This power gives the United States much more influence on the policy decisions about the Internet than any other country.

---

<sup>72</sup> See also *supra* text accompanying note 33; *cf. Report on Redlegation of the .af Top-Level Domain*, *supra* note 9.

<sup>73</sup> See *Bylaws for Internet Corporation for Assigned Names and Numbers*, Art. XI, § 2(1), at <http://www.icann.org/general/bylaws.htm> (Oct. 13, 2003) (“Governmental Advisory Committee”).

<sup>74</sup> See *supra* note 11 (discussing nations’ demands for a transfer of influence over the internet from the United States to the United Nations); World Summit on the Info. Soc’y, *Building the Information Society: A Global Challenge in the New Millennium*, ¶¶ 50, 64, at <http://www.itu.int/wsis/docs/geneva/official/dop.html> (Dec. 12, 2003).

<sup>75</sup> See *supra* note 39.

<sup>76</sup> Employed techniques limit to some extent all countries’ control. For example, IP addresses and domain names are not strictly related to countries, and therefore of limited use for the enforcement of territorially organized rules. See *L’Association Union des Etudiants Juifs de France v. Yahoo! Inc., T.G.I. Paris, Ordonnance de référé du 20 novembre 2000, RG 00/05308*, available at <http://www.foruminternet.org/telechargement/documents/tgi-par20001120.pdf> (Nov. 20, 2000); *League Against Racism and Antisemitism v. Yahoo! Inc., County Court of Paris (2000)*, available at <http://www.cdt.org/speech/international/001120yahoofrance.pdf> (Nov. 20, 2000) (providing an English translation); *cf. Revue Lamy Droit des affaires* 2001, No. 34, No. 2158]. But if all states agreed, they could force a change of the employed technology to

## II. LIMITATIONS OF SOVEREIGNTY

Having established the U.S.'s power over the Internet in Part I, this Article will proceed in Part II to search for a legal basis for this power that could be used by the U.S. to defend against other countries' challenges to American control.<sup>77</sup> An examination of ownership is crucial because other legal doctrines like sovereignty do not provide a legal basis for such a far-reaching power. A country's sovereignty provides it with the authority to exercise jurisdiction, which is the competence to regulate conduct or the consequences of events.<sup>78</sup> Territoriality is the primary basis for jurisdiction; as all persons and things within the territory of a state fall under its territorial authority, each state normally has legislative, judicial, and executive jurisdiction over them.<sup>79</sup> Therefore, given the A-root-server's location in the United States, at first glance the United States would appear to have the power to regulate the root file.

Apart from the questions of how the server and the intangible data stored on it relate to each other, and to what extent the location of the data is a useful consideration, such a claim based on territorial authority ends at the U.S. borders but the effect of U.S. regulation is a worldwide one.<sup>80</sup> Other countries may claim that their sovereignty gives them a say in Internet regulation because of the effect on their territory. Two legal doctrines support such a position of other countries. The first one is self-determination, a fundamental human right of peoples.<sup>81</sup> The second one is the

---

overcome such obstacles. Smaller countries that resist could be cut off. Yet the likelihood of such an agreement among all powerful countries is low.

<sup>77</sup> See *supra* note 11 and accompanying text.

<sup>78</sup> See 1 OPPENHEIM'S INTERNATIONAL LAW 456-57 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

<sup>79</sup> 1 *id.* at 458.

<sup>80</sup> The argument that any state control lacks legitimacy in cyberspace as presented by Barlow, Johnson and Post calls into question only the legitimacy of actions of a single state that affect all "netizens," but not collective actions taken by all states, because the social contracts of all states combined grant such legitimacy. John Perry Barlow, *Declaration of the Independence of Cyberspace*, at [http://www.missouri.edu/~rhetnet/barlow/barlow\\_declaration.html](http://www.missouri.edu/~rhetnet/barlow/barlow_declaration.html) (Feb. 9, 1996); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

<sup>81</sup> See, e.g., International Covenant on Civil and Political Rights, G.A. Res. 2200A, U.N. GAOR, 21st Sess., Supp. No. 16, at 52, art. 1, U.N. Doc. A/6316 (1966), 999

effects doctrine, which grants a country jurisdiction if its territory is affected by events taking place outside its territory.<sup>82</sup> The effects doctrine has been advocated by the United States in antitrust law against many objections by other countries. The rationale behind it is to secure sovereignty in a world of international trade. This rationale behind the effects doctrine applies to the Internet because all countries are substantially affected by the root. The counterargument that other countries could reinforce their sovereignty by “pulling the plug” from the Internet is unconvincing, because the same argument applied in the realm of antitrust law would destroy the basis for the effects doctrine there because a country can elect to stop participating in global trade. Overall, non-Americans are just asking that those who exercise the control over the Internet derive their just powers from the consent of all the governed.<sup>83</sup> In the end a sovereignty-based approach encounters severe problems because of conflicting sovereignty.

### III. DOES OWNERSHIP LEGITIMIZE U.S. POWER?

#### A. *Property Claim*

The property claim that could provide a legal basis for U.S. control over the Internet is that the Internet is an American

---

U.N.T.S. 171, 6 ILM 368; International Covenant on Economic, Social and Cultural Rights, G.A. res. 2200A, 21 U.N. GAOR 21st Sess., Supp. No. 16, at 49, art. 1, U.N. Doc. A/6316 (1966), 993 U.N.T.S. 3, 6 ILM 360.

<sup>82</sup> See *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 795–96 (1993); *United States v. Alum. Co. of Am.*, 148 F.2d 416, 443 (2d Cir. 1945); *Hoffman-La Roche, Ltd. v. Empagran S.A.*, 124 S. Ct. 2359 (2004); *Empagran S.A. v. F. Hoffman-LaRoche*, No. 01-7115, 2004 U.S. App. LEXIS 13431 (D.C. Cir., June 21, 2004); Address by U.S. Attorney General Griffen Bell to the Law Counsel of Australia (July 17, 1978), in *EXTRATERRITORIAL JURISDICTION 4* (Alan Vaughan Lowe ed., 1983). The effects doctrine is controversial. 1 *OPPENHEIM’S INTERNATIONAL LAW*, *supra* note 78, at 460. Where actions of states are at issue, the acts of state doctrine hinders a direct application. The second requirement of the effects doctrine is the intent to affect the second country. The United States has such an intent because they do willfully exercise worldwide control.

<sup>83</sup> *Cf.* THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

“thing.”<sup>84</sup> The Internet was invented by scientists who were working for the U.S. government. However, the fact that the Internet was built and funded by the U.S. government does not necessarily translate into a property right and a right to worldwide control.<sup>85</sup>

The following section applies traditional legal concepts in order to examine if they provide a basis for a claim of American ownership. A government need not own something in order to have the power to regulate it; the object in question only needs to be within its territory. A U.S. claim solely based on location, however, like jurisdiction over territory, is problematic due to the effect of U.S. decisions on the self-determination of other countries, as has been discussed in Part II, and because of the virtual nature of the Internet—the root file and the protocols are intangible and the notion of “cyberspace” is nothing but an often misleading metaphor for many connected computers.<sup>86</sup>

### *B. Ownership of Tangible Things*

Ownership is the collection of rights allowing one to use and enjoy property, including the right to convey it to others and the

---

<sup>84</sup> See *supra* note 12. A similar idea is that IEEE owns the Ethernet address space because it was a standard formalized by IEEE. See MUELLER, *supra* note 17, at 28.

<sup>85</sup> Some doubt is already raised by the fact that the most important part of today’s Internet, the World Wide Web, was developed by the Englishman Tim Berners-Lee at the research institution CERN (in Geneva, Switzerland), which is funded by European taxpayers. See JANET ABBATE, *INVENTING THE INTERNET* 214 (1999); TIM BERNERS-LEE, *WEAVING THE WEB* (1999).

<sup>86</sup> Intangible “things” do not have a location even if they are saved on a storage device. The latter is only an edition of the intangible “thing.” A common description of the Internet is that it is not a thing. Rather it is entirely virtual and consists of the software protocols TCP/IP. MUELLER, *supra* note 17, at 6; Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 552 (1998); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003) (discussing the problems with the metaphor of cyberspace); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003). The power of the metaphor derives from the fact that, at first glance, it replaces a complicated analysis along new lines of thinking. Lawyers struggle to resist metaphors because they rely on language without a formal method, which forces them to make all assumptions and conclusions obvious. The reason is that lawyers deal with the world in all its complexity and cannot reduce the world to formal models that deviate from reality.

right to exclude others from use.<sup>87</sup> Ownership is not restricted to the country in which it was originally acquired. Most conflict-of-laws questions regarding real property and tangible movables (chattels) are governed by the *situs* rule, which applies the law of the state in which the thing in question is located.<sup>88</sup> If tangible movables are brought to another country, however, this second country applies its law only to facts occurring after they crossed the border.<sup>89</sup> Therefore the *situs* rule leads to the application of the second country's property law, but the second country normally will recognize the ownership position gained in the first country.

The last point is decisive. If property law applied to the Internet and the United States owned it accordingly, then other countries would have to accept American ownership and control. But U.S. ownership depends on the extent to which the Internet can be perceived as tangible movables or real property. The root file is a set of data, which does not fall within the realm of land or tangible movables, and is thus precluded from protection under property law.<sup>90</sup> The same is true for the TCP/IP protocols, which are algorithms but not tangible goods. It then follows that the U.S. could not have a title of ownership for the root file and TCP/IP because they are not tangible movables. However, the backbone consists of tangible things like fiber optic cables, and the United States was the owner of the original backbone. Nevertheless, the United States privatized the original Internet backbone "NSFNET" in 1995, and parts of today's Internet backbone were built, and are owned by, entities spread over the world, mostly by the leading telecommunications corporations of the world and national telecommunications carriers.<sup>91</sup> In addition, the local loop has

---

<sup>87</sup> 63C AM. JUR. 2D Property §§ 26–27 (2002).

<sup>88</sup> See EUGENE F. SCOLES ET AL., CONFLICT OF LAWS 943–45, 963–65 (3d ed. 2000). That the considerations with respect to tangible movables are often more complicated is not decisive here because the point is universal recognition in other countries.

<sup>89</sup> RESTATEMENT (SECOND) OF CONFLICT OF LAWS: PROPERTY § 247 (1971) ("Interests in a chattel are not affected by the mere removal of the chattel to another state. Such interests, however, may be affected by dealings with the chattel in the other state.").

<sup>90</sup> The property right in the data does not depend on the ownership of the server where the data are stored. Froomkin, *supra* note 20, at 44–45 (pointing out that the server belongs to NSI-Verisign).

<sup>91</sup> See Barry M. Leiner et al., *A Brief History of the Internet*, Internet Society, at <http://www.isoc.org/internet/history/brief.shtml> (Dec. 10, 2003); European Commission,

always been the property of local telecommunication carriers. Therefore, rules of ownership for tangible things do not support a claim for American ownership of the Internet.<sup>92</sup> Because a claim of U.S. ownership based on tangible movables fails, an analysis of a claim of a U.S. property right based on intellectual property law is necessary.

### C. U.S. Intellectual Property Law

The potential claim of invention by the United States leads to the law for inventions and creative works. This Article first examines U.S. intellectual property law to determine whether, and to what extent, protection could have been, or even was, granted. Second, it explores international treaties on intellectual property to determine to what extent the United States could have demanded the recognition of U.S. property rights in other countries.

#### 1. TCP/IP and Copyright

The TCP/IP protocols are implemented as computer programs. The threshold for copyright protection is originality.<sup>93</sup> Original means that (i) the work owes its origin to the author, i.e., the work was independently created by the author as opposed to copied from other works, and (ii) that the work possesses at least some minimal

---

Decision, June 28, 2000, Case COMP/M.1741, MCI WorldCom/Sprint, ¶¶ 16, 22; Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89 (2001).

<sup>92</sup> Courts sometimes apply (real) property law to cyberspace. *See, e.g.*, *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997) (applying trespass to chattels to e-mail spam); LG Berlin, *Neue Juristische Wochenschrift* [NJW] 55 (2002), 2569 (applying § 1004 BGB (German civil code)). Even if one agrees with the application here, there is a crucial difference between this application and the qualification of the entire Internet. In spam cases, for example, hardware is at least affected and this may justify the application of property law to certain problems. But this does not alter the fact that the Internet in its entirety can hardly be characterized as tangible. *See supra* note 86 (discussing metaphors for the internet).

<sup>93</sup> 17 U.S.C. § 102 (a) (1976, 2000). The text cites to the U.S.C. of 1976 to show that the relevant parts of the provisions were in force in 1981 and also to the current U.S.C. to show that the analysis would be the same today.

degree of creativity.<sup>94</sup> At least some of the protocols in question certainly have sufficient originality to meet this test because they are one of the first descriptions of a new technology.

However, the functionality of the protocols could make them noncopyrightable. This issue arises out of a basic conflict within copyright law. On the one hand, there is the longstanding principle of copyright law that functional elements are not copyrightable. On the other hand, computer software, which is always functional,<sup>95</sup> has at least been copyrightable since 1981.<sup>96</sup> This conflict can be interpreted as a problem of the relationship between patent law and copyright law or as part of the distinction between idea and expression.<sup>97</sup> According to the idea-expression dichotomy, copyright protection is limited to particular expressions of ideas, but does not extend to any idea as such.<sup>98</sup> The idea-expression dichotomy is difficult to apply because the result depends on the applied level of abstraction. There is no clear solution to this problem. Some courts apply an abstraction-filtration-comparison test to filter out unprotectable elements,<sup>99</sup> but this does not provide a clear answer, since the appropriate level of abstraction is uncertain.<sup>100</sup> The particular way the TCP/IP protocols are expressed in the documents RFC 791 and RFC

---

<sup>94</sup> Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991); 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.01[A] (2003).

<sup>95</sup> In the end, all purely expressive elements in a computer program are superfluous.

<sup>96</sup> Congress intended so when it adopted two changes in 1980 that added a definition of computer program and substituted a new section 117 in the Copyright Act. An Act to amend the patent and trademark laws, Pub. L. No. 96-517, § 10, 94 Stat. 3015, 3028 (1980) (codified as amended with irrelevant later changes at 17 U.S.C. §§ 101, 117 (1982, 2000)); *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1247-48 (3d Cir. 1983).

<sup>97</sup> See Lloyd L. Weinreb, *Copyright for Functional Expression*, 111 HARV. L. REV. 1149, 1178-81 (1998).

<sup>98</sup> 17 U.S.C. § 102(b) (2000); *Baker v. Selden*, 101 U.S. 99 (1879).

<sup>99</sup> *Computer Assocs. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 706 (2d Cir. 1992); cf. 4 NIMMER & NIMMER, *supra* note 94, § 13.03[F].

<sup>100</sup> See Mark A. Lemley, *Convergence in the Law of Software Copyright?*, 10 HIGH TECH. L.J. 1, 20-23 (1995). If one considers "how to build a network" as the idea, then TCP/IP is one of several possible expressions. At a lower level of abstraction, however, the analysis becomes that of the "packet based network," and then the concept of TCP/IP is one of only a few expressions, for which the merger doctrine would apply to deny copyright protection. *Morrissey v. Procter & Gamble Co.*, 379 F.2d 675 (1st Cir. 1967) (applying merger doctrine).

793,<sup>101</sup> i.e., the text of these documents as such, is certainly copyrightable.<sup>102</sup> That means that literal copying of the text would infringe a copyright. But does the copyright also cover the concepts expressed in these texts and prohibit their implementation in software code?

An argument against such copyright protection is that the documents RFC 791 and RFC 793 describe a concept that can be implemented (“expressed”) in computer code in many ways and copyright does not protect a concept (“idea”) but only the code or user interface of particular implementations (“expressions”). The protocols just describe the functionality the actual programs must have; they are not executable computer programs themselves. There is a step missing from the protocols to a running program, and there are several ways to implement the concept. This can be compared to an instructional book that describes how to write a new type of novel. Copyright should not limit other people’s freedom to write such novels as long as they do not use expressions from the instructional book. To hold otherwise would mean that a copyright owner owns a monopoly of a group of expressions of an idea independently from the used expressional elements. Similarly, the protocols express very abstract ideas and therefore patent law (discussed below) and not copyright law would be the right body of law to grant protection.

U.S. copyright law does not protect the protocols as ideas.<sup>103</sup> The fact that the expression of these ideas in the RFCs is at least

---

<sup>101</sup> See *supra* text accompanying note 56.

<sup>102</sup> Whether the missing copyright notice on these two RFCs invalidated the copyright depends on the number of copies distributed. 17 U.S.C. § 405 (2000). After they had been made available via the Internet and had been downloaded very often, the copyright was very likely invalidated.

<sup>103</sup> The issue of U.S. government works is therefore not decisive. Copyright protection is not available for any work prepared by an officer or employee of the U.S. government as part of that person’s official duties, but the U.S. government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise. 17 U.S.C. §§ 101, 105 (1976, 2000). Some people involved in the development of TCP/IP were government employees; others were contractors. The protocols could be U.S. government works, commissioned works, or commissioned works derived from government works. The beginnings of RFC 791 (IP) from 1981 and RFC 793 (TCP) from 1981 include: “prepared for Defense Advanced Research Projects Agency . . . by Information Sciences Institute . . .” Thus it should be presumed that the protocols are

partly copyrightable does not mean that other people are prohibited by copyright law from using the ideas, i.e., to implement the protocols by writing computer code according to the principles laid down in the RFCs.

## 2. TCP/IP and Patent Law

U.S. patent law states as the first threshold for patent protection, that one must “invent[] or discover[] [a] new and useful process.”<sup>104</sup> Whether computer programs are patentable subject matter was contested for a long time. One obstacle was the “mental steps doctrine” that holds that no patent can be obtained for any method in which all of the steps could be performed in the mind of a person, but the doctrine is no longer applied with respect to computer software.<sup>105</sup> Today, a mathematical formula (abstract idea or algorithm) is no longer absolutely barred from patent

---

commissioned works. The copyright could be held by the contractor or be transferred to the government. Such a commission with accompanying transfer would not violate 17 U.S.C. § 105 (1976, 2000). See *Schnapper v. Foley*, 667 F.2d 102 (D.C. Cir. 1981); *United States v. Washington Mint, LLC.*, 115 F. Supp. 2d 1089 (D. Minn. 2000). Knowledge of the contracts would facilitate the evaluation. But the contracts between U.S. government agencies like DARPA and private contractors like the company BBN are not available. BBN did not keep a copy of the contract from 1969. Phone Conversation of the Author with the Librarian of BBN (spring 2001). A Freedom of Information Act request was answered with a no record decision (02-F-1560): “The Defense Advanced Research Projects Agency (DARPA) found no records responsive to your request concerning the contract called “DARPANET” between DARPA (IPTO) AND BBN (Bolt Beranek Newman) from 1969. . . . For example, the first research contract associated with the DARPANET was awarded to BBN under contract number DAHC15-69-1769, Interface Message Processors, 2 January 1969. . . . The contract requested was administered by Defense Supply Service-Washington (DSSW) number DAHC15-69-C-1769. However, a query to that organization revealed that contracting records from that time frame have been destroyed.” It is reasonable to assume that the U.S. government made sure that all possible rights belong to it. All in all, 17 U.S.C. § 105 (1976, 2000) is not a decisive factor in copyright protection.

<sup>104</sup> 35 U.S.C. § 101 (1976, 2000).

<sup>105</sup> See 1 DONALD S. CHISUM, CHISUM ON PATENTS § 1.03[6] (2003); A. Samuel Oddi, *Assault on the Citadel: Judge Rich and Computer-Related Inventions*, 39 HOUS. L. REV. 1033, 1045–50 (2002); Richard S. Gruner, *Intangible Inventions: Patentable Subject Matter for an Information Age*, 35 LOY. L.A. L. REV. 355, 400–03 (2002); James P. Chandler, *Patent Protection of Computer Programs*, 1 MINN. INTELL. PROP. REV. 33, 42–48 (2000).

protection.<sup>106</sup> Only a mathematical algorithm in isolation (“abstract”) is not patentable, whereas a process that applies an equation to a new and useful end (“practical application”) is patentable.<sup>107</sup> The test today is whether there will be a useful, concrete, and tangible result.<sup>108</sup> The TCP/IP protocols result in the transport of data and therefore meet this standard. However, it is unclear whether in 1981, when the invention of the protocols was made public, a court would have held the protocols to be patentable subject matter because the legal standard was an open question at that time.<sup>109</sup>

The other requirements for patentability are much less questionable. The necessity of novelty<sup>110</sup> is easily fulfilled since the packet-based network technology was groundbreaking.<sup>111</sup> This also shows that the protocols were non-obvious, another requirement for obtaining a patent.<sup>112</sup> Finally, the requirement of enablement<sup>113</sup> was met by the documentation in RFCs.

Setting aside the uncertainty about whether the protocols were patentable subject matter in 1981, one requirement for patent protection was definitely missing: the filing of patent applications. It would have been necessary to file the patent application within a year after the RFCs were published in September 1981.<sup>114</sup> No application was filed and thus the statutory bar applies. As a result, the protocols have fallen into the public domain.<sup>115</sup>

---

<sup>106</sup> *State St. Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1373–75 (Fed. Cir. 1998); Wesley L. Austin, *Software Patents*, 7 TEX. INTELL. PROP. L.J. 225, 252 (1999).

<sup>107</sup> *AT&T Corp. v. Excel Communications, Inc.*, 172 F.3d 1352, 1356–57 (Fed. Cir. 1999).

<sup>108</sup> *Id.* at 1357; *State St.*, 149 F.3d at 1373.

<sup>109</sup> *Cf. Diamond v. Diehr*, 450 U.S. 175, 193 (1981) (Stevens, Brennan, Marshall, and Blackman, J.J., dissenting).

<sup>110</sup> 35 U.S.C. § 102 (1976, 2000).

<sup>111</sup> Doubts could only arise from prior publications, such as V. Cerf & R. Kahn, A *Protocol for Packet Network Intercommunication*, 22 IEEE TRANSACTIONS ON COMMUNICATIONS 637 (1974), or earlier RFCs.

<sup>112</sup> 35 U.S.C. § 103 (1976, 2000).

<sup>113</sup> *Id.* § 112 (1976, 2000).

<sup>114</sup> *Id.* § 102(b) (1976, 2000).

<sup>115</sup> Even if a property right had been obtained, the patent term would have already expired because even today’s term of 20 years has passed since the last possible filing date of September 1982. 35 U.S.C. §§ 102(b), 154(a)(2) (2000). The term was changed

Therefore, TCP/IP protocols are protected neither by U.S. copyright law nor by U.S. patent law.

### 3. Root File and Copyright

The remaining ways for the United States to argue for the existence of a property right include: (1) patent and copyright protection of the root file, (2) patent protection of the DNS, and (3) trademark protection of the namespace. Whether the root file is protected by copyright or whether it is an unprotectable compilation of facts depends on the text of the file. As this Article has already established, the root file assigns to each TLD a name server.<sup>116</sup> Thus at first glance, the root file just reports facts. But because only the root file makes a particular name server the definitive source of information on a particular TLD, the correspondence between the listed domain names and the listed IP addresses on that name server was not only reported by the root file but was created by it.

This could be dispositive in light of *Feist*, a case that dealt with copyright protection for a telephone directory.<sup>117</sup> The Supreme Court stated in *Feist* that the critical distinction is between copyrightable creation and non-copyrightable discovery<sup>118</sup> and held that copyright protection should not be granted in the case because the data did not owe its origin to the copyright claimant. “Rather, these bits of information are uncopyrightable facts; they existed before Rural reported them . . . .”<sup>119</sup>

The wording of *Feist* can lead to misunderstandings. One could argue that whether the facts existed before is decisive and conclude by an *argumentum a contrario* that created facts are copyrightable. As applied to the root file, this conclusion would lead to the following argument: the assignment of this TLD to that name server did not exist before. Therefore, the facts in the root file indeed owe their origin to the United States, through ICANN

---

from 17 to 20 years by Uruguay Round Agreements Act, Pub. L. 103-465, § 532, 108 Stat 4809 (1994) (codified as amended at 35 U.S.C. § 154 (a)(2) (2000)).

<sup>116</sup> See *supra* text accompanying note 24.

<sup>117</sup> *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991).

<sup>118</sup> *Id.* at 347.

<sup>119</sup> *Id.* at 361.

and NSI-Verisign, and they thereby meet the threshold for protection. However, such an argument would be a misinterpretation of *Feist* because the decisive facts in *Feist* and the case of the root file are the same. The facts of the type “this name to this number/server” in *Feist* were indeed created by the telephone company when it assigned its customers the telephone numbers, as the Supreme Court indicated.<sup>120</sup> The only difference between *Feist* and the root file is that in *Feist*, the creation of the fact by assigning the numbers happened before the facts were collected and reported in the phone book, while in the case of the root file, the creation (assignment) and the report took place in one step. This difference does not affect the level of creativity and is therefore insignificant.

The Supreme Court’s wording is insufficient to decide cases in which someone seeks copyright protection for facts they created and cannot be relied upon to extend copyright protection to facts created by a party. The Supreme Court ignored this problem as the contradiction between its following statements show: “[r]ural then assigns them a telephone number”<sup>121</sup> versus “this data [names and telephone numbers] does not ‘owe its origin’ to Rural.”<sup>122</sup> The facts owe their origin to Rural, but facts as such are independent from the issue of creation, never copyrightable. According to a careful reading of *Feist*, the facts in the root file themselves are not copyrightable and only the compilation of them could be subject to copyright protection.

A copyrightable compilation requires a creative arrangement of the facts.<sup>123</sup> The arrangement of the facts within the root file is mainly alphabetical and otherwise random, i.e. non-creative.<sup>124</sup> Thus the root file is not protected under U.S. copyright law.<sup>125</sup>

---

<sup>120</sup> *Id.* at 343 (“Rural then assigns them a telephone number.”).

<sup>121</sup> *Id.*

<sup>122</sup> *Id.* at 361.

<sup>123</sup> *Id.* at 358, 363.

<sup>124</sup> Even if there were an order because of technical necessities, there would be no creativity. Furthermore, the issue would arise of who the potential copyright holder would be. See *supra* note 103; Froomkin, *supra* note 20, at 45 (focusing on whether the root file “belongs” to the government). There are additional legal issues because, for example, a transfer of a work created as nongovernmental work to the government means

#### 4. Root File, DNS and Patent Law

The root file would have to be a process with useful, concrete, and tangible results to qualify for patent protection, but the root file is only data that is processed as input and does not represent the process itself, which is generated by the name servers.<sup>126</sup> Thus the root file is protected neither by copyright law nor by patent law in the United States.

Instead of the root file, one could focus on the DNS for protection.<sup>127</sup> The DNS meets today's basic requirements for patent protection because it directs users using a domain name to the corresponding IP address and therefore represents a software-based process with useful, concrete, and tangible results. But it is at least uncertain whether it would have been patentable in 1983 when the specifications of the original DNS were published in RFCs,<sup>128</sup> because the patentability of computer programs was an unsettled issue at that time.<sup>129</sup> As with TCP/IP, there is no report about a patent application and the protection would have already expired.<sup>130</sup> For these reasons, the DNS is not protected by patent law.

#### 5. Other Protection of the Root File

Another approach would be to claim ownership not of the technical concept of the DNS, but of the namespace consisting of the domain names as such, i.e., the use of all names ending with a TLD like ".com", at least for network purposes. Such a claim does not easily fit into the system of intellectual property law because

---

that the government holds a copyright. The contract between the U.S. government and NSI (and ICANN) has some influence on the characterization as a governmental work.

<sup>125</sup> See Froomkin, *supra* note 20, at 45 ("The root file lacks sufficient originality to be copyrightable, nor is it the sort of collection likely to be entitled to a compilation copyright.").

<sup>126</sup> See RFCs 1034–35 for process and necessary algorithms.

<sup>127</sup> See RFCs 882–83 (both published Nov. 1983).

<sup>128</sup> See *supra* note 127.

<sup>129</sup> Cf. *supra* text accompanying note 109.

<sup>130</sup> Cf. Paul V. Mockapetris & Kevin J. Dunlap, *Development of the Domain Name System*, 18 ACM SIGCOMM COMPUTER COMM. REV. 123, 124 (Aug. 1988) (Initial design of the DNS was specified in RFCs 882–83 and the current specifications are quite similar to the original definitions.).

namespaces have not been a traditional concern of lawmakers. Copyright law does not provide protection because of the functional nature of the namespace as an address system. In addition, there are concerns about the level of creativity because one could argue that such a namespace is, in the end, a creation of facts that is unprotectable according to *Feist*. Patent law could only cover the DNS as a technical application, but a namespace as such cannot be held patentable because it does not fall within the type of inventions and discoveries patent law was intended for, instead falling in the realm of non-patentable abstract ideas. A namespace as such is neither a tangible product<sup>131</sup> nor a process that produces a tangible result.

Another possibility is trademark law, which protects a word, name, or symbol used to identify and distinguish goods or services from those manufactured or sold by others, and to indicate the source of the goods or services, even if the source is unknown.<sup>132</sup> Today it is established that a second-level domain such as “unitedairlines” in “unitedairlines.com” can qualify as a trademark. The threshold for trademark protection is that the second-level domain is more than part of the function of locating a Web site,<sup>133</sup> but additionally identifies and distinguishes the source of goods or services.<sup>134</sup>

Under U.S. law, a TLD is unlikely to qualify as a trademark or a service mark. To qualify for trademark protection, ICANN or the United States would have to specify the registration of domain names as a service they offer, which would be difficult because both ICANN and the United States are not acting as registries or registrars. Furthermore, the District Court for the Central District of California rejected the trademark claim of a company that

---

<sup>131</sup> Cf. 1 CHISUM, *supra* note 105, § 1.02.

<sup>132</sup> See 15 U.S.C. § 1127 (2000). Because the acquisition of a trademark is not bound to the law at the time of first use, it is appropriate to look at the current law. The change in the definition with respect to unknown sources did not even alter the law. See 1 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION, § 3:9 (4th ed. 2003).

<sup>133</sup> Examples of something that merely locates include a street address or telephone number.

<sup>134</sup> 1 MCCARTHY *supra* note 132, § 7:17.1; *Brookfield Communications, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1055 (9th Cir. 1999).

wanted to act as registry and registrar for the TLD “.web”, because neither domain name registrants nor website visitors recognized “.web” as indicator of source, but only as the type of Web site designated.<sup>135</sup> The court held that no registrant believed that .web indicated a certain registrar because there was more than one place to register.<sup>136</sup> TLDs do not indicate a source to a potential Web site visitor; only the second-level domain names communicate information as to a source. Thus, the court concluded that a TLD was not protected by trademark law.<sup>137</sup>

Another approach would be to view ICANN or the U.S. government as the source of all domain names of which the TLD is a part, for example all domain names ending with .org. For at least some TLDs, there is only one registry and one can see the registrars as merely acting as intermediaries like retailers.<sup>138</sup> From the perspective of potential domain name holders, the second-level domain is then a product and not merely a source identifier, and the attached TLD is the trademark of the maker of the product, which would be ICANN or the registry as licensee.<sup>139</sup> The (low) likelihood that the average registrant would know that the U.S. government or ICANN is the source of the TLD is not important because the source can be unknown.<sup>140</sup>

If the alleged identifier is a necessary part of the product, however, it could conflict with the doctrine of functionality, which excludes functional matters from trademark protection.<sup>141</sup> In the *TrafFix* decision, the Supreme Court used the following definition: “In general terms, a product feature is functional, and cannot serve

---

<sup>135</sup> *Image Online Design, Inc. v. Core Ass’n*, 120 F. Supp. 2d 870, 876 (C.D. Cal. 2000). The court additionally qualified the alleged trademark as generic. *Id.* at 879; see also Patent and Trademark Office, *Marks Composed, in Whole or in Part, of Domain Names, Examination Guide No. 2-99*, at <http://www.uspto.gov/web/offices/tac/notices/guide-299.htm> (Sept. 29, 1999).

<sup>136</sup> The court may have confused the terms registrar and registry. There is one registry for a TLD but several registrars.

<sup>137</sup> *Image Online Design*, 120 F. Supp. 2d at 878.

<sup>138</sup> See MUELLER, *supra* note 17, at 261–62.

<sup>139</sup> On the level of web surfing consumers, only the second-level domain matters. Any consumer confusion as to the source of the TLD cannot be claimed because it does not matter for the Web site visitors.

<sup>140</sup> The likelihood would probably be different for a TLD “.coca-cola”.

<sup>141</sup> See 15 U.S.C. § 1052(e)(5) (2000); 15 U.S.C. § 1125(a)(3) (2000).

as a trademark, if it is essential to the use or purpose of the article or if it affects the cost or quality of the article.”<sup>142</sup> The design of a domain name serves the purpose of, and is essential to, locating and directing people to an Internet address. Therefore, a TLD is functional because it indicates what (sub-) namespace the domain names belong to.<sup>143</sup>

Moreover, there are important limits in the scope of trademark protection. Even if trademark protection of a TLD would, in general, be possible as some argue,<sup>144</sup> trademark law would not grant a monopoly for the entire domain, that is, for all names that include the TLD. Trademark protection for a word like “.web” would not forbid others from using the word in other distinctive combinations like “animal.web”, and in most cases would not even prevent the use of the same word for another class of goods or services. Even the protection of famous trademarks (which would require that many consumers think of a company being the source of “.com” domain names) has limitations. Trademark protection protects the use of a word in a particular context but not all words derived from it.<sup>145</sup> Trademark law does not provide an opportunity to protect a group of words as such.<sup>146</sup>

Finally, one could look to tort and unfair competition law for a right to exclusive use and control.<sup>147</sup> However, a claim of

---

<sup>142</sup> *TrafFix Devices, Inc. v. Marketing Displays, Inc.*, 121 S. Ct. 1255, 1261 (2001) (internal quotations omitted).

<sup>143</sup> The special situation is that the product itself is an identifier and the TLD is a functional part of it because it directs computers to the IP address. Furthermore, one has to ask whether this case differs from other identifiers. Could a telephone company really claim a trademark for all 1-800 numbers because the company is the source of a group of phone numbers with particular properties?

<sup>144</sup> See MUELLER, *supra* note 17, at 261–62 (arguing that it is possible to have just one registry for a TLD, but many registrars, acting merely as intermediaries, delivering a registry’s service to the public as do retailers).

<sup>145</sup> With respect to the class of products or services, there is no class like domain names or namespaces within which any use of derived words would be prohibited.

<sup>146</sup> IP addresses are just functional numbers. Therefore, the IP address space meets the requirements of trademark protection even less so than TLDs.

<sup>147</sup> With respect to the use of names, one can distinguish between an alternative use, which does not hinder functionality, e.g., use of same numbers for spare parts, and an alternative use that hampers the original use. Here, an alternative use of the same names would disturb the DNS because data would be sent to the wrong computer although the same name is used.

misappropriation under state law would fail due to federal preemption, because federal law does not grant copyright, patent, or trademark protection for a namespace as such.<sup>148</sup>

## 6. Summary of U.S. Intellectual Property Law

Intellectual property rights were not acquired for the Internet's technologies and key resources under U.S. law because first, they were to a large extent unprotectable, and second, filing requirements were not fulfilled. Moreover, patent protection would have expired by now. In conclusion, U.S. intellectual property law does not support a claim of U.S. ownership.

### *D. International Intellectual Property Law*

Assuming for the sake of argument that the technology behind the Internet qualified for intellectual property protection in the United States, would other countries be obliged to accept American "ownership"? Intellectual property law is governed by the territorial principle. Every country's power to grant a monopoly for an invention or a work of art ends at its borders. The general rule is that a country does not recognize intellectual property rights granted in another country, but independently decides this issue.<sup>149</sup> The reason for this policy is a nation's sovereignty: to hold otherwise would mean a country could severely interfere with another country's policy. Every nation is therefore in principle free to accept or reject an American monopoly depending on its own policy.

---

<sup>148</sup> RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (1995); see *Int'l News Serv. v. Assoc'd Press*, 248 U.S. 215 (1918); *McKevitt v. Pallasch*, 339 F.3d 530, 534 (7th Cir. 2003) (holding that *Int'l News* is now only state law: "That decision no longer is legally authoritative because it was based on the federal courts' subsequently abandoned authority to formulate common law principles in suits arising under state law though litigated in federal court."); *Bd. of Trade v. Dow Jones & Co.*, 456 N.E.2d 84, 88-89 (1983).

<sup>149</sup> This is reflected in all international treaties on intellectual property. See Paris Convention for the Protection of Industrial Property, art. 4*bis*, Mar. 20, 1883, revised July 14, 1967, 828 U.N.T.S. 305 [hereinafter Paris Convention], available at <http://www.wipo.int/clea/docs/en/wo/wo020en.htm>; Berne Convention for the Protection of Literary and Artistic Works, art. 5(2), Sept. 9, 1886, revised July 24, 1971, 1161 U.N.T.S. 3, 31 [hereinafter Berne Convention], available at <http://www.wipo.int/clea/docs/en/wo/wo001en.htm>.

International treaties like the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs)<sup>150</sup> require minimum protection of intellectual property and thereby limit national sovereignty.<sup>151</sup> Therefore, other nations have to grant the United States a monopoly for a limited period of time if the root file and TCP/IP are covered by these minimum standards.<sup>152</sup>

### 1. Software Patents in Treaties

The only treaty that could impose a duty to grant software patents is TRIPs, which states that “patents shall be available for any inventions, whether products or processes, in all fields of technology.”<sup>153</sup> This broad definition and the fact that computer software is not part of the list of exceptions in Article 27 TRIPs for which member states can exclude patentability, weigh in favor of a duty to grant software patents. The better arguments, however, hold against such an interpretation.<sup>154</sup> In most countries, “pure”

---

<sup>150</sup> Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND, 33 I.L.M. 1125, 1197 (1994) [hereinafter TRIPs Agreement].

<sup>151</sup> The obligation to grant national treatment, which is part of many international treaties, does not affect the principle of territoriality because it only hinders an arbitrary application of the national law based on nationality and does not deal with the recognition of foreign rights. See Paris Convention, *supra* note 149, art. 2; Berne Convention, *supra* note 149, art. 5(1); TRIPs Agreement, *supra* note 150, art. 3.

<sup>152</sup> It is not convincing to use other countries' national laws as an argument because other countries are free to lower protection to the required minimum level and are then not obligated to accept any U.S. property right for something not meeting the minimum level even if some countries with higher levels of protection would have problems taking once acquired rights away.

<sup>153</sup> See TRIPs Agreement, *supra* note 150, art. 27.

<sup>154</sup> Cf. Jerome H. Reichman, *Universal Minimum Standards of Intellectual Property Protection under the TRIPs Component of the WTO Agreement*, in INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPs AGREEMENT 21, 41–42 (Carlos María Correa & Abdulqawi Yusuf eds., 1998); Carlos M. Correa, *Patent Rights*, in INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPs AGREEMENT 189, 199–200 (Carlos María Correa & Abdulqawi Yusuf eds., 1998); MARKUS NOLFF, TRIPs, PCT AND GLOBAL PATENT PROCUREMENT 65 (2001); Charles R. McManis, *Taking TRIPs on the Information Superhighway*, 41 VILL. L. REV. 207, 220, 248, 286 (1996); John T. Soma et al., *Software Patents: A U.S. and E.U. Comparison*, 8 U. BALT. INTEL. PROP. L.J. 1, 67 n.329 (2000); Andreas Heinemann, *Trade-Related Aspects of Intellectual Property Rights*, in FROM GATT TO TRIPs 401, 414 (Friedrich-Karl Beier & Gerhard Schricker eds., 1996).

software patents were not granted at the time the treaty was finalized and signed.<sup>155</sup> To require patent protection of software in TRIPs would have been such a major policy shift that an explicit statement would be necessary to conclude that software patents are included in the minimum standards agreed upon in TRIPs. Such a narrow interpretation is strongly supported by the copyright provisions of TRIPs that deal with the same policy question. Traditionally, copyright law did not cover software. Article 10 of TRIPs explicitly mandates a change from that policy. It is unconvincing that the same type of policy change applies to both patents and copyrights, where it was only made explicit for copyright. It is more likely that the signatory countries did not agree upon such a policy shift in patent law. Therefore, countries still have considerable latitude under TRIPs in deciding to what extent software-related inventions are patentable.<sup>156</sup> Furthermore, these issues are moot because the TRIPs agreement was signed in 1994, well after TCP/IP was published in 1981, and has, according to Article 70, no retroactive power. Additionally, even if we were to assume that TCP/IP had to be patentable under TRIPs, nobody has ever filed patent applications for TCP/IP or the DNS<sup>157</sup> and even if they did the patents would have expired by now.

---

<sup>155</sup> See RAINER SCHULTE, PATENTGESETZ MIT EUROPÄISCHEM PATENTÜBEREINKOMMEN § 1, No. 98 et seq. (6th ed 2001); Proposal for a Directive of the European Parliament and of the Council on the Patentability of Computer-Implemented Inventions, 2002 O.J. (C 151 E) 129, at <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/ce151/ce15120020625-en01290131.pdf>.

<sup>156</sup> NOLFF, *supra* note 154, at 65.

<sup>157</sup> Patent protection outside the United States is complicated by the requirement of absolute novelty and the lack of a one-year grace period (*cf.* 35 U.S.C. § 102(b)) in other countries. *E.g.*, Convention on the Grant of European Patents (European Patent Convention), arts. 54–55, Oct. 5, 1973, 1065 U.N.T.S. 255, 13 I.L.M. 268, 270; Patentgesetz in Deutschland [Patent Act of Germany], § 3, v. 1981 (Bundesgesetzblatt, Teil I [BGBl. I] S.1). Any publication of the invention before the filing of a patent application bars the invention from protection. TRIPs and other treaties do not affect this. The IETF procedure to publish standard proposals makes it impossible to get patent protection if no patent application is already pending.

## 2. Copyright Treaties

Copyright protection of computer programs is not part of the Berne Convention<sup>158</sup> but was introduced by Article 10 of TRIPs and Article 4 of the WIPO Copyright Treaty.<sup>159</sup> The root file is not an executable computer program but only a compilation of facts. Therefore the root file could only be protected under provisions that provide protection for compilations of data. Article 10(2) of TRIPs and Article 5 of the WIPO Copyright Treaty require protection only for compilations of data that constitute intellectual creations by reason of the selection or arrangement of their contents. The selection of the domains in the root file is simply a consequence of their existence and the arrangement is in alphabetical order. Thus, the root file does not meet the minimum standard of Article 10(2) of TRIPs and Article 5 of the WIPO Copyright Treaty.<sup>160</sup>

The TCP/IP protocols again raise the issue of the distinction between idea and expression because Article 9(2) of TRIPs<sup>161</sup> and the Agreed Statements Concerning the WIPO Copyright Treaty (“Concerning Article 4”) exclude ideas as such.<sup>162</sup> Therefore, as

---

<sup>158</sup> Paul Katzenberger, *TRIPs and Copyright Law*, in *FROM GATT TO TRIPs* 59, 84 (Friedrich-Karl Beier & Gerhard Schricker eds., 1996). Software is neither protected by the Universal Copyright Convention, Stockholm, July 24, 1971, 25 U.S.T. 1341, 943 U.N.T.S. 178, which is according to its Article XVII and Annex 1 subsidiary to the Berne Convention.

<sup>159</sup> WIPO Copyright Treaty, Geneva, Dec. 20, 1996, S. TREATY DOC. NO. 105-17 (1997), 36 I.L.M. 65, available at <http://wipo.int/treaties/en/ip/wct/index.html>.

<sup>160</sup> The United States cannot even claim protection for the root file in the European Union. Council Directive 96/9/EC on the Legal Protection of Databases, 1996 O.J. (L 77) 20. Article 11 of this directive limits the protection to residents of the European Union and protection is only extended to residents of other countries that entered into a special agreement with the European Union because the European Union requires reciprocity. However, the United States does not protect databases of this kind and did not enter into a special agreement with the European Union. *Cf. supra* note 152.

<sup>161</sup> See TRIPs Agreement, *supra* note 150, art. 9(2) (“Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.”).

<sup>162</sup> Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, *Agreed Statements Concerning the WIPO Copyright Treaty* (“Concerning Article 4”), at <http://www.wipo.int/documents/en/diplconf/distrib/96dc.htm> (Dec. 23, 1996) (“The scope of protection for computer programs under Article 4 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPs Agreement.”).

already discussed, there is no copyright protection against the free implementation of the underlying concept.

There are also other reasons preventing copyright protection. The protocols TCP and IP were introduced in September 1981 but TRIPs was signed in 1994 and has, as already mentioned, no retroactive power.<sup>163</sup> Article 13 of the WIPO Copyright Treaty, however, refers to Article 18 of the Berne Convention and is therefore retroactive. But not all nations have signed the WIPO Copyright Treaty<sup>164</sup> and the claim would not work with non-signatory nations. It is also doubtful that the United States would still be able to enforce copyright claims because free use was never contested. Finally, assuming all countries had to grant copyright protection to the United States, this right and the claim for derived legitimacy would not last forever but only for about sixty years from now.

### 3. Trademark and Tort Law

Trademark law follows the territorial principle,<sup>165</sup> but the provisions of the Paris Convention introduce some minimum standards for trademark protection.<sup>166</sup> However, they do not require any state to protect a TLD with all its second-level domains as a trademark or service mark for the United States or ICANN, just as other countries do not have any obligation to protect and accept a U.S. claim to such a namespace based on tort or unfair

---

<sup>163</sup> See RFCs 791 (IP, Sept. 1981), 793 (TCP, Sept. 1981).

<sup>164</sup> See *Contracting Parties*, <http://www.wipo.int/treaties/en/documents/pdf/s-wct.pdf> (Oct. 27, 2004).

<sup>165</sup> *Vanity Fair Mills, Inc. v. T. Eaton Co.*, 234 F.2d 633, 640 (2d Cir. 1956) (stating that the Paris Convention was premised on the principle that each nation's law shall have only territorial application); see Paris Convention, *supra* note 149, art. 6(3). Sometimes an extraterritorial application is claimed. Yelena Simonyuk, *The Extraterritorial Reach of Trademarks on the Internet*, 2002 DUKE L. & TECH. REV. 9. However, the cases involved are exceptional and their findings are often based on international treaties and not on extraterritorially applied national laws; furthermore it is often just a question of wording whether to call the application of a law extraterritorial.

<sup>166</sup> See Paris Convention, *supra* note 149, art. 6*sexies*; Madrid Agreement Concerning the International Registration of Marks, art. 4, Apr. 14, 1891, revised July 14, 1967 (Stockholm), 828 U.N.T.S. 389, available at [http://www.wipo.int/madrid/en/legal\\_texts/trtdocs\\_wo015.html](http://www.wipo.int/madrid/en/legal_texts/trtdocs_wo015.html).

competition law, because namespaces were not intended to be protected.

### CONCLUSION

Neither rules of property nor rules of intellectual property support the claim that the United States owns the worldwide Internet.<sup>167</sup> This has important consequences for the related idea of the Internet being an American gift to the world. A gift is in the narrow legal sense a voluntary transfer of property by one person to another without any consideration or compensation therefore.<sup>168</sup> Thus, it is hard to argue a gift approach because of the lack of merits of an ownership claim. So while the United States gave the world free access to the technology, the United States cannot claim special power over it, since it did not have a property right.<sup>169</sup>

Finally, it is instructive to consider the Olympic Games, an example of a global public good, in order to demonstrate the limitations of national power with respect to global public goods. The Olympic Games affect many people and are to some extent similar to a network good such as the Internet: the more countries that participate, the more valuable the games are. They are organized by a private entity, the International Olympic Committee (IOC).<sup>170</sup> States do not have any rights in the decision-making and

---

<sup>167</sup> This claim somewhat resembles what Vaughan Lowe called “one of the most imaginative, and least successful, attempts to extend the scope of jurisdiction”—the attempt to assert jurisdiction on the basis of the “nationality” of technology—a concept unknown in international law—by U.S. export regulations during the cold war. *Vaughan Lowe, Jurisdiction in INTERNATIONAL LAW* 346–47 (Malcom D. Evans ed., 2003); see also *European Communities: Comments on the U.S. Regulations Concerning Trade with the U.S.S.R.*, 21 I.L.M. 891 (1982).

<sup>168</sup> 38 AM. JUR. 2D *Gifts* § 1 (2004).

<sup>169</sup> It is not possible to argue that physical access to the Internet was a gift because the United States could not withhold the worldwide Internet. The United States only had two options: to hinder the development of the worldwide network, or to help develop it by granting worldwide access. But the United States could not give the worldwide network to the world because it did not exist before the world participated. Nevertheless, other countries should consider acknowledging the prominent role that the United States played in the international development of the Internet.

<sup>170</sup> International Olympic Committee, *Olympic Charter*, chs. 6(3), 7(1), 33, at [http://multimedia.olympic.org/pdf/en\\_report\\_122.pdf](http://multimedia.olympic.org/pdf/en_report_122.pdf) [hereinafter *Olympic Charter*] (Sept. 1, 2004).

are not members of the IOC, which is comprised of natural persons who are not allowed to accept mandates from governments.<sup>171</sup>

The key symbols of the Olympics are the rings and the flame.<sup>172</sup> The Olympic flame is kindled in Olympia, Greece.<sup>173</sup> Considering the history of the Olympic Games, which were originally invented in ancient Greece and then reinvented in 1894,<sup>174</sup> Olympia is the natural location with a unique symbolic value for the flame. Olympia, which gives the flame its special meaning, is in this sense a rare resource comparable to the root file. Furthermore, Greece has the same legal power to define the property rights within its borders as the United States does. Nevertheless, not many would say that because the Olympic Games were originally a Greek “thing,” and because Olympia and the flame-lighting are in Greece, Greece has a justified claim for demanding every fourth Olympic Games take place in Greece. Factual control, location, and origin in a country do not always translate into a legitimate claim of control on a worldwide scale.<sup>175</sup> This claim is lost if the resource in question develops from a national good into a global public good.

No matter which entity should govern the Internet, a simplistic ownership claim has rather limited merits and heuristic value.<sup>176</sup>

---

<sup>171</sup> *Id.*, chs. 16.1.1, 16.1.5. Compared to the Internet, the Olympic Games are a true case of private ordering with no state claiming a special role. It is an example of rule by private entities without any state officially interfering. This is not to say that the IOC is a success story.

<sup>172</sup> Countries grant the IOC trademark protection. *See* Nairobi Treaty on the Protection of the Olympic Symbol, adopted Sept. 26, 1981, 1863 U.N.T.S. 367, available at [http://www.wipo.int/treaties/en/ip/nairobi/trtdocs\\_wo018.html](http://www.wipo.int/treaties/en/ip/nairobi/trtdocs_wo018.html).

<sup>173</sup> *Olympic Charter*, *supra* note 170, ch. 13.1.

<sup>174</sup> *See id.*, pmb1.

<sup>175</sup> This comparison is not affected by the differences in the level of power of Greece and the United States over the Olympic Games and the Internet, and in the importance of participating in the Olympic Games and the Internet.

<sup>176</sup> A separate issue is whether the United States has reason to hesitate to transfer its power to ICANN, the history of which is at least not very encouraging.